Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy guidance for the education sector

This guidance focuses on the unique needs of those working within and on the frontline of the education sector.

Whether you're a teacher, a principal, an administrator, a member of a school board, a speech language therapist, a guidance counsellor, operate an ECE service, or are a service provider providing services to learners, this guidance has been created for you.

In this guidance we use "education provider" to mean any organisation that is on the frontline of the education sector. This includes schools, ECE services and service providers. This guidance may also be useful to other non-education sector agencies working with children and young people.

In this guidance:

How to use this guidance

This guidance has been designed to be easy to navigate and read, and simple to apply in your day-to-day work. While it focuses on the privacy of learners, much of the guidance also applies to other personal information you may hold (e.g. personal information about staff and parents).

This guidance is set out in chapters that focus on a specific area of the Privacy Act 2020 (the Privacy Act). Each chapter identifies relevant information privacy principles (IPPs), or sections of the Privacy Act, then provides guidance on how to apply those provisions in practice. Each chapter also provides links to additional resources and tools to help you embed good privacy practices into your day-to-day work.

This guidance also includes chapters on specific 'topics' such as the rights of children and young people, education technology and health and learning support information. We recommend that you read through the guidance completely, but if you are short on time, you can navigate directly to the chapter or topic of interest.

This guidance focuses on the Privacy Act, but other legislation such as the Education and Training Act 2020, the Public Records Act 2005, the Oranga Tamariki Act 1989 or the Family Violence Act 2018 also apply to learner information. Where

appropriate, the guidance refers to other applicable legislation and how it works with the Privacy Act.

While this guidance aims to help you make good privacy decisions with confidence, it cannot resolve every privacy issue that may arise. Some situations may require a more detailed analysis of the Privacy Act or other legislation. When these situations arise, you should seek legal advice.

This guidance builds on our free online toolkit Poupou Matatapu, which provides a framework for setting up and managing your privacy program.

Acknowledgements

This guidance was developed with the help of our education expert advisory group, who made sure this guidance was practical and useful for the education sector.

Children, young people and their personal information

Children and young people are special – a taonga to be nurtured and supported as they complete their journey through to adulthood.

The children and young people of today will grow to become our leaders, our workforce, our parents and our stewards of the future. Their experiences growing up will shape and foster the adults they will become.

All children and young people in New Zealand navigate their way through an education journey – it is an ever-present part of their development to adulthood and beyond. Teachers, support staff and others working with children and young people in the education sector contribute towards that development in many ways.

A child or young person's information is an intrinsic part of who they are – it represents their past, their present and their future. Misuse of that information can create lasting impacts for a child or young person. Understanding how to protect and respect a child or young person's personal information and implementing good privacy practices will ensure all children and young people in New Zealand have positive privacy experiences throughout their education journey.

Privacy rights of children and young people

Domestic and international law together create a framework of privacy protections for children.

The Privacy Act 2020

The Privacy Act is the primary law that governs personal information, and it applies to everyone regardless of age.

The Privacy Act requires that you take particular care when collecting personal information from children and young people. It also gives children and young people the same rights as adults to request and correct their information, and authorise collection, use, and disclosure of their information. They can also make a complaint if they believe their privacy has been breached.

Very young children, or children and young people with cognitive disabilities, won't necessarily be able to exercise their privacy rights on their own. In these cases, a representative can support a child or young person to exercise their rights or exercise a child or young person's rights on their behalf.

For most children and young people, their ability to exercise their rights will increase as they grow older. A child or young person's age and their cognitive maturity will be important considerations when collecting, using or sharing a child or young person's information, or managing requests or complaints.

United Nations Convention on the Rights of a Child

New Zealand is a signatory to the United Nations Convention on the Rights of a Child (UNCRC).

The UNCRC is an international treaty that outlines the fundamental rights of every child. UNCRC defines children as all persons under the age of 18. The UNCRC recognises children need special protection of their human rights, including their right to privacy, due to their age and stages of development.

There are two key parts of the UNCRC that are relevant to ensuring a child or young person's privacy is protected and respected:

- the best interests of the child consideration, and

- the right to privacy set out in Article 16.

Interpretation of the information privacy principles set out in the Privacy Act 2020 should always be considered with the best interests of the learner in mind.

Best interests of the Child

The UNCRC contains a general principle (Article 3) that a child has the right to have their best interests assessed and considered as a primary consideration.

What this means in practice is that whenever there is a decision to be made that will affect a child or young person the decision-making process should include an evaluation of the possible impact (both good and bad) of the decision on the child or young person.

The best interests of a child or young person is a dynamic concept - what is in the best interests of the child or young person will depend on the circumstances.

Right to Privacy

Article 16 of the UNCRC makes it clear that children and young people have the right to privacy, including informational privacy.

Additional resources

The UN Committee on the Rights of the Child General Comment provides a detailed interpretation of the best interests of a child requirement in the UNCRC. You can access this resource here: UN General Comment: Best Interests of the Child.

The Privacy Act 2020 and personal information

Education providers play an important role in how children and young people experience privacy on a day-to-day basis.

Information collected about learners creates and builds a story about their educational journey, including their health, wellbeing and family circumstances. A learner's educational story is part of who they are, and something they carry for the rest of their lives.

Getting privacy right builds trust and empowers learners to understand and exercise their privacy rights effectively. Getting privacy wrong can have a significant long-term impact on a learner and their family.

The Privacy Act 2020

The Privacy Act 2020 (the Privacy Act) governs how organisations collect, use, store and share **personal** information.

The Privacy Act ensures that:

- people know when their personal information is being collected
- personal information is used and shared appropriately
- personal information is kept safe and secure
- people can access and correct their personal information.

The Privacy Act applies to **all** education providers and their staff, including members of a board that governs your organisation (for example, members of a school board or board of directors).

What is personal information?

Personal information is any information that tells us something about an identifiable individual.

Personal information doesn't need to include someone's name. It only needs to include enough information to tell you or someone else who they are.

Personal information in the education sector

What constitutes personal information in the education sector is broader than you may think.

Examples of personal information include:

Enrolment information

- Names and contact information for the learner, family, siblings and key contact people.
- NSN and other unique identifiers.
- Demographic information; sex and gender, ethnicity, age.
- Medical and health information including immunisation records, medical conditions, allergies and disabilities.

Attendance and wellbeing information

- Attendance records.
- Absence responses and regular attendance plans.
- Health and wellbeing related information including pastoral care records.
- Disciplinary actions.

- Information about a learner's homelife.

Learning information

- Individual education plans.
- Timetables.
- Progress and achievement records.
- Career and pathway planning information.
- Internet usage and device login information.
- Photos, videos and audio recordings.

What form can personal information take?

Personal information can take any form – it can be written, digital or hardcopy, or contained in images.

Information you receive from a learner or another person during a conversation can also be personal information. For example:

- a staff member talking to you during lunchtime about a learner and issues with their home life
- information shared at a staff meeting
- a principal of another school calling you to discuss a learner that is looking to enrol at that school
- a meeting with a parent where the parent shares information about their concerns of bullying by other learners
- interviewing other people as part of an investigation or disciplinary process.

Personal information can also be contained within your organisation's documents such as written correspondence, meeting minutes (staff, parent and board meetings), reports, newsletters, emails, voice messages, photos and videos, and text messages.

When you receive personal information verbally from another person that you may need to use or refer to later (e.g. used to inform a decision about a learner) then you should make a record of it.

Personal information received verbally is subject to the Privacy Act 2020.

Other information received verbally is subject to the Official Information Act 1982 (OIA) if your organisation is subject to the OIA.

Information privacy principles (IPPs)

There are 13 information privacy principles (IPPs) in the Privacy Act that govern the collection, use, storage and sharing of personal information.

This guidance works through the application of these IPPs to help you make good privacy decisions and ensure your learner's privacy is protected and respected.

General information about the 13 IPPs can be found here: Office of the Privacy Commissioner | Privacy Act 2020 and the Privacy Principles.

Information used solely for personal, family or domestic purposes

In most cases, the Privacy Act does not apply to the domestic affairs of individuals unless the collection, use or sharing of the personal information involved is highly offensive.

This means that activities by a parent such as taking photos or videos of their child (that may also include images of other learners) at a school or ECE service event and posting them online are not subject to the Privacy Act.

Privacy is everyone's responsibility

Leaders and managers must have a clear understanding and effective oversight of privacy and deliberately make protecting and respecting a learner's privacy a priority.

Accountability vs responsibility

It's important to understand who in your organisation is accountable and who is responsible for protecting the privacy of your learners' personal information.

Accountability means:

- accepting ownership for protecting personal information and privacy risks
- assurance that processes are in place to ensure your privacy policy and associated processes are being followed
- being able to explain decisions that impact a learner's privacy and why they were made
- making sure things are fixed if they have gone wrong.

Accountability plays a fundamental role in ensuring learners' personal information is protected and respected. Leaders and managers of education providers are accountable for ensuring learners' personal information is managed in accordance with the Privacy Act 2020.

Responsibility means:

- making sure your privacy policy and processes are implemented and followed
- reporting privacy matters to leaders and managers (e.g. privacy complaints or breaches).

All staff are responsible for ensuring a learner's privacy is protected and respected. That means that everyone should know about their organisation's privacy policy, how to implement requirements of the policy and how to implement the requirements of the Privacy Act in practice.

Some staff (for example, your privacy officer or other subject matter experts) will be responsible for implementing and embedding the privacy policy and processes set by leaders and managers and ensuring leaders and managers are aware of privacy matters that require consideration.

Accountability example – Schools

School boards are accountable for ensuring the school complies with the Privacy Act.

Principals or other senior school staff are responsible for implementing and embedding the school's privacy policy and processes and reporting privacy related matters to the board.

All school staff are responsible for knowing, understanding and applying the school's privacy policy in their day-to-day work.

Accountability example – ECE services

Business owners (or board of directors if you have one) are accountable for ensuring an ECE service complies with the Privacy Act.

Centre Managers or other senior ECE service staff are responsible for implementing and embedding the ECE service's privacy policy and processes and reporting privacy related matters to the business owner (or board of directors).

Accountability example – Service providers

The person accountable for compliance with the Privacy Act will depend on the structure of the service provider e.g. a non-government organisation (NGO), a charity, a registered company, a trust or an incorporated society etc.

The service provider's senior staff are responsible for implementing and embedding the provider's privacy policy and processes and reporting privacy related matters to the board.

All staff working for the service provider are responsible for knowing, understanding and applying the providers privacy policy in their day-to-day work.

Setting up your privacy function

The Privacy Commissioner has developed Poupou Matatapu to help organisations understand what good privacy practice looks like. The first Pou focuses on how to set up and maintain good privacy governance.

The Governance Pou will help you understand what privacy governance is and how to establish your privacy governance function. If you already have a privacy governance function in place, the Governance Pou can help you to identity any gaps and see where you could make improvements.

For information about how to set up your privacy governance function see: Office of the Privacy Commissioner | Governance.

The New Zealand School Boards Association (NZSBA) provides services to school boards including support, advice and professional development. The NZSBA resource centre provides a number of resources for school boards including responsibilities under the Privacy Act.

You can access the NZSBA resource centre here: Help for Boards.

Getting privacy right in practice

The following actions are fundamental to embedding good privacy practice and ensuring compliance with the Privacy Act:

- development, implementation and review of a fit for purpose privacy policy and processes
- ensuring the collection, use, storage and disclosure of learner's personal information complies with the Information Privacy Principles (IPPs)
- ensuring IT systems are fit for purpose and adequately protect learner's personal information
- managing and responding to requests for information appropriately and in a timely manner
- managing and responding to privacy breaches, including mandatory breach notification where appropriate
- managing and responding to privacy complaints
- requiring all staff to undertake privacy training annually
- appointing a privacy officer.

Fit for purpose privacy policy and privacy statements

A privacy policy is a document that sets out how your organisation collects, uses, shares and protects personal information. Having a privacy policy demonstrates that you know what information you collect and hold, understand what you can use that information for, and have implemented appropriate measures to keep that information safe.

Privacy statements, sometimes referred to as Privacy notices, are more often used for specific collections of personal information. A privacy statement is a good way to provide learners (and their parents) with the more detailed, collection-specific information necessary for them to make an informed decision about providing you with their personal information in those specific circumstances.

You can also refer to your privacy policy in your collection-specific privacy statement – this will enable learners (and their parents) see how the specific collection aligns with your organisation's general privacy practices.

For more information about privacy policies and privacy statements see: Chapter 8 Keeping Learners and parents informed.

Privacy complaints process

Complaints can be an indicator of potentially problematic privacy practices. Creating and implementing a robust complaints process enables you to manage complaints effectively and receive meaningful privacy complaint reports.

Awareness and understanding of privacy complaints provides an opportunity to review privacy processes and practices and make improvements where necessary.

For detailed guidance on managing privacy complaints see Chapter 14: Managing Privacy Complaints.

Privacy incident register and response plan

When a privacy breach occurs, it can create a high stress environment for all people involved. Having a documented privacy incident response plan in place helps people know what they need to do, when they need to do it, and how they should do it.

Creating and implementing a Privacy Incident Register enables awareness and oversight of privacy incidents and provides an opportunity to review privacy processes and practices and make improvements where necessary.

For guidance on privacy incidents see Chapter 15: Privacy Incidents.

Regular privacy reporting

Regular and meaningful reporting of privacy issues to the governance function is critical to maintaining oversight of privacy issues. You can't deal with privacy matters effectively or in a timely manner if you aren't aware of them.

Members of the governance function should make privacy a standing agenda item at all governance meetings and set clear expectations of what privacy related information you want reported. At a minimum, privacy reporting should include:

- privacy incidents and breaches
- privacy complaints received and managed
- privacy requests received and managed
- proposals for new technology or systems that use personal information
- report back on privacy matters raised by the governance function in the last reporting period
- privacy training conducted in the last reporting period.

Privacy officers

The Privacy Act requires education providers to have at least one privacy officer who is responsible for managing privacy matters.

A privacy officer helps ensure that a privacy policy and processes are in place and that staff are aware of them. A privacy officer can also help identify and resolve privacy matters that arise in a quick and effective manner. No special training or qualification is required to be privacy officer, but they do need to understand the requirements of the Privacy Act.

Having a privacy officer can also help you build a positive privacy culture within your organisation and develop trusted relationships with your learners and their parents.

For more information about privacy officers and their responsibilities see: Office of the Privacy Commissioner | Information for Privacy officers.

Training for privacy officers

It is important that privacy officers have the knowledge necessary to fulfil their functions. Providing access to privacy training is a good way to help support your privacy officer feel confident in their role.

Privacy officers can access free online privacy training here: Office of the Privacy Commissioner | E-learning. There are also organisations that provide specific training for privacy officers.

Privacy officers can also join the 'Privacy Officers Round Table' (PORT), an active network of privacy officers in Auckland, Wellington, and Christchurch. Members from the private and public sectors meet regularly. Read more about each PORT chapter and contact an organiser.

Practical actions for privacy officers

In practice, a privacy officer can fulfil some of their responsibilities under the Privacy Act by incorporating the following actions into their workplans:

- Report regularly to senior leadership (school board, board of directors, or business owners) about privacy matters including breaches and complaints.
- Manage or assist with managing privacy concerns or complaints.
- Complete an audit of the way personal information is collected, used, shared and stored.
- Complete a review of forms (e.g. consent and enrolment forms) used to collect personal information to ensure compliance with IPPs 1 – 4.
- Complete regular reviews of your organisations privacy policy and privacy statement.

Example – Privacy reporting to school board

O is the privacy officer for a local primary school. Each month O prepares a report for the school board outlining privacy issues that have occurred. O's report covers privacy complaints that the school have received, privacy incidents, privacy training that has been provided to school staff, and other general privacy matters.

As part of its privacy policy, the school encourages its staff to report all privacy incidents to the privacy officer. The school board notices that over the last several months there has been an increase in privacy incidents relating to the use of email by staff. In the majority of cases, incorrect email addresses have been recorded as the cause. The school board is pleased that the staff feel safe to report these incidents, but the increase in incidents is a concern.

After some discussion around appropriate measures to mitigate the privacy risks associated with the incidents the school board agrees to implement the send delay function of the school's email software. The send delay function delays the sending of emails for two minutes, enabling staff to identify where an incorrect email has been identified and correct it before the email is sent.

The school board advises the school principal and privacy officer of the decision, and requests that confirmation of the implementation of the send delay function is provided at the next board meeting.

Privacy and confidentiality

Privacy and confidentiality both play a part in protecting learners' information.

Often these terms are used interchangeably, but they are distinct concepts and should be considered separately.

Privacy

The rights of a learner to exercise some control over the collection, use and disclosure of their personal information.

Privacy is about a person's right to control their information, activities and personal space. With respect to information, privacy is about a person's right to determine what personal information about them is collected, used, and shared by others.

Privacy is not just about keeping information private, it's about respecting a learner's mana, and protecting their information from unauthorised intrusion.

The Privacy Act sets out obligations on all organisations that collect, use and share personal information to ensure personal information is respected and protected.

Confidentiality

An education provider's obligation to protect certain information from unauthorised access and disclosure

We use confidentiality to mean:

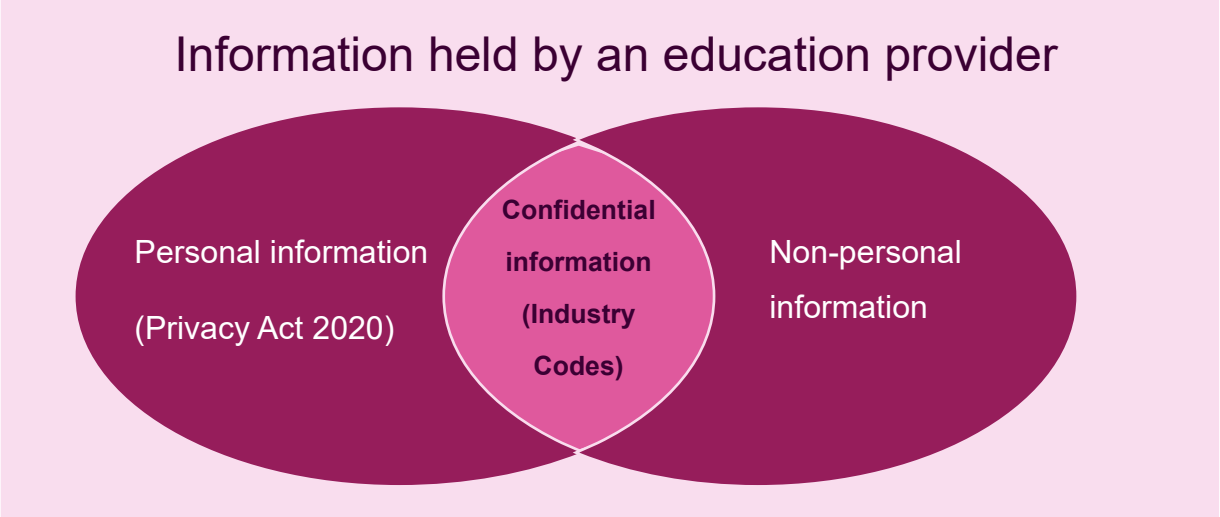
- the ethical duty that someone might have because of their profession
- the legal duty that someone might have because of their profession

- the contractual duty someone might have because of their contract with an education provider.

These duties require that certain information is protected from unauthorised access, use and disclosure. Confidentiality is particularly relevant in certain professional settings e.g. between a counsellor and their patient, a teacher and a learner, a social worker and a client, or a lawyer and their client.

Confidential information

Confidential information can include personal and non-personal information. Confidential information that is personal information will also be covered by the Privacy Act.



There isn't a definition of confidential information. It will be defined differently across different organisations, businesses, professions and sectors. For example:

- From an employment perspective, employees have a general duty to keep their employer's information confidential, but employment contracts will often contain clauses that define how that information will be managed and how confidentiality will apply even after an employee no longer works for that employer.

- When delivering education-related services to learners, terms and conditions related to the delivery of that service will state what information collected will be treated as confidential information and how it will be managed.
- Industry Codes of Conduct or Codes of Ethics may also define what information is considered confidential and place obligations on professionals working in that industry to ensure that information is protected from unauthorised access and disclosure.

Maintaining confidentiality is not just a legal or ethical obligation – just like protecting privacy, it is a fundamental aspect of building and maintaining trust. Learners and their parents will feel more comfortable sharing personal information when they understand when it will be kept confidential.

Confidentiality and the Privacy Act 2020

Where personal information is also confidential information, often the obligations to protect that information will reflect the obligations set out in the Privacy Act, or in the case of health information, those set out in the Health Information Privacy Code 2020.

For more information about health information see Chapter 9: Health and Learning Support information.

However, confidentiality is typically narrower in scope – it involves specific agreements, industry codes or policies to protect information deemed to be confidential from unauthorised access and disclosure. Therefore, obligations of confidentiality may restrict access to, and disclosure of, confidential personal information further than the exceptions set out in information privacy principle (IPP) 11 of the Privacy Act.

	PRIVACY	CONFIDENTIALITY
Legal Framework	Privacy Act 2020	Contracts, Code of Professional Conduct
Type of Information	Personal Information	Personal and non-personal information
Legal Authority to Share	IPP11 Exceptions • Serious threat • Law enforcement • Authorisation (consent) • Other IPP 11 exceptions	Exceptions to Confidentiality, which might include: • Serious risk to a person's health or life • Required by law • Consent

Table setting out the legal framework, the type of information, and authority to share information that applies with respect to both privacy and confidentiality.

Exceptions to confidentiality

There may be situations where you need to share confidential information. An exception to confidentiality must have a legal authority that permits the sharing of that information.

Common exceptions to confidentiality include:

- where there are significant health or safety concerns for the learner (e.g. the IPP11 serious threat exception, section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act).
- where the learner has authorised (consented) to the information being shared (e.g. the IPP11 authorisation exception).
- where the sharing of the information is required by another law.

You'll generally find exceptions to confidentiality reflected in professional codes (e.g. Code of Ethics or Codes of Conduct) or contracts to provide services.

When advising a learner (or their parents where appropriate) that specific information, or categories of information, will be kept confidential you should always clearly inform them of the exceptions to that confidentiality i.e. the circumstances in which you may share that information.

Privacy and confidentiality in practice

The following section covers a number of codes that operate within the education sector that include obligations of confidentiality.

It is important to note that codes can be created by legislation or voluntarily by an industry organisation.

Codes created by legislation

Some codes are created under legislation (i.e. they are secondary legislation), which means everyone subject to the code must comply with it.

Codes created by legislation in the education sector include:

- Teachers Code of Professional Responsibility (section 485, Education and Training Act 2020)
- Code of Conduct for State Board Members (section 166, Education and Training Act 2020)
- Social Workers Registration Board (SWRB) Code of Conduct (section 105, Social Workers Registration Act 2003).

Teachers Code of Professional Responsibility

The Teachers Code of Professional Responsibility sets out the ethical behaviour expected of every teacher. It applies to all certificated teachers and those who have been granted a Limited Authority to Teach, in every role and teaching context.

The Teachers Code of Professional Responsibility is supported by a set of Standards. The Standards are a benchmark of how to comply with this code. Because the Standards are not legislation, they do not limit the Privacy Act.

To read more about the Teachers Code of Professional Responsibility see: Our Code, Our Standards Teaching Council of Aotearoa New Zealand.

Code of Conduct for State School Board Members

All state and state-integrated school board members are required to comply with the Code of Conduct for State School Board members.

Objective 11 of this code requires all board members to maintain confidentiality when they receive non-public information gained in the course of their duties and can only use the information for the purposes for which it was obtained.

Objective 11 reflects the requirements of the Privacy Act around the use and disclosure of personal information but provides specific restrictions on the use and disclosure of all information obtained by school board members, whether it is personal information or non-personal information. The Code of Conduct for State School Board Members does not replace or change the requirements of the Privacy Act.

To read more about the Code of Conduct for State School Board Members see: Code of conduct for school boards - Ministry of Education.

Example – Media Inquiry to school board member

M is a school board member for XYZ Primary School. The school has recently experienced issues with tensions between local gang members at school pick up time. These tensions have created a number of safety issues for the school, learners, and parents/caregivers waiting to pick up their children. The school board is currently with working with local Police to deescalate the tensions and keep everyone safe.

M is out shopping when they are approached by a local reporter. The reporter asks M for information about the gang tensions, whether the gang members have children at the school, and what the school is doing to keep learners and others safe during school pick up times.

Can M share information with the reporter?

The Privacy Act applies to personal information, which would include information relating to any learners who are children of the gang members. In the circumstances, there are no exceptions to IPP 11 requirements that would apply so M cannot share any personal information about learners with the reporter.

M is also subject to the Code of Conduct for State School Board Members. The Code makes it clear that M must comply with all statutory requirements relevant to their role, which includes responsibilities under the Privacy Act. The Code also provides that all non-public information M obtains through their role as a board member must be kept confidential. This means that in the circumstances, M cannot share any information about the gang tensions or any discussions between the school and the Police with the reporter unless M has been authorised to do so by the Board.

The Board will have a process for responding to media requests, and M should refer the reporter to that process.

Social Workers Registration Board Code of Conduct

The Social Workers Registration Board (SWRB) Code of Conduct sets out the minimum standards of integrity and conduct that apply to registered social workers.

Principle 7 of this code (Respect the client's privacy and confidentiality) provides that all registered social workers are expected to:

- protect the privacy of the client's personal information

- make it clear that all information gained in the course of the social worker/client relationship is confidential
- inform clients of the extent of confidentiality and the situations where information may need to be shared.

The SWRB Code of Conduct's requirements reflect the requirements of the Privacy Act and Health Information Privacy Code – they don't replace or change the requirements of the Privacy Act.

The SWRB Code of Conduct's requirements don't override the information sharing provisions set out in section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act.

For more information about sharing information for the protection of children and young people see our guidance: Office of the Privacy Commissioner | Sharing information to protect the wellbeing and safety of children and young people.

Example – Social Worker in Schools (SWiS)

G is registered social worker employed by a Non-Government Organisation (NGO) as a Social Worker in Schools (SWiS) social worker. G works with a number of high-risk learners across different primary and intermediate schools. Each learner that G works with has been referred to them with the consent of the learner's parent.

When getting consent to provide a service to the learner, learners (and their parents) are informed that all information shared with them will be kept confidential but that certain information about the learner may be share with:

- the school to assist the school to provide appropriate learning supports
- relevant agencies and organisations if the learner's safety and wellbeing is at risk.

During a meeting with a learner, G also notices that the learner has bruising on their arms and legs. G asks the learner about the bruises, and the learner discloses to G that their parents get a bit angry with them sometimes.

Can G share the information the learner has disclosed to them?

The Family Violence Act 2018 provides the legal authority to share personal information to help ensure that a person is protected from family harm. Sharing information for one of the specified purposes under the Family Violence Act would not result in a breach of the Privacy Act or the SWRB Code of Conduct.

Under the SWRB Code of Conduct the information the learner has disclosed to G is considered confidential personal information because it has been described as confidential to the learner and their parents in the consent to provide services process. However, as part of the consent process, the learner and their parents were also informed that the obligation of confidentiality is not absolute. If there are concerns for the learner's safety and wellbeing, the social worker can share this information with appropriate agencies and services – in this case, using section 20 of the Family Violence Act.

In this case, G could share relevant personal information about the learner with an appropriate family violence agency to help protect the learner from further harm.

To read more about the Code etc see: SWRB website: Resources | Social Workers Registration Board.

Industry codes

Some codes are created by industry organisations, where members of that organisation are required to comply with the code as part of their membership with that organisation.

Members codes created by industry organisations in the education sector include the New Zealand Association of Counsellors (NZAC) Code of Ethics.

New Zealand Association of Counsellors Code of Ethics

The NZAC Code of Ethics states that counsellors shall treat all communications between a counsellor and client as confidential unless the client gives consent to particular information being shared. The Code of Ethics is a voluntary code for counsellors who choose to become members of NZAC. It does not limit or change the Privacy Act.

The NZAC Code of Ethics also says that limits to confidentiality should only be made to reduce risk to the client and then states what those exceptions are.

The confidentiality rules in this code reflect the requirements of the Privacy Act (and for any health information, the Health Information Privacy Code) but narrow the range of exceptions for when information collected from a client can be shared e.g. only with consent of the individual or when there is significant risk to the individual.

The NZAC Code of Ethics'requirements don't override the information sharing provisions set out in section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act.

For more information about sharing information for the protection of children and young people see our guidance: Office of the Privacy Commissioner | Sharing information to protect the wellbeing and safety of children and young people.

To read more about the NZAC Code of Ethics see: Code of Ethics - NZAC.

Example – School guidance counsellor

K is a guidance counsellor employed by a High School. K has been meeting with 14-year-old J regularly over the last six months. J has been experiencing difficulties in their home life which have impacted her ability to concentrate at school and develop

relationships with other learners. There is currently no immediate risk of danger to J's safety or wellbeing. J has also made it clear to K that they do not want any of the information they have shared with K disclosed to other people within the school.

J's teacher has approached K to seek information about J. J's teacher believes that if they understand what was happening for J, they would be able to provide better support to J in the classroom.

Can K share any information about J with J's teacher?

Under the Privacy Act, K is not able to share any personal information with J's teacher unless one of the exceptions in IPP 11 (or Rule 11 for health information) apply. In the circumstances set out above, there is no exception to IPP11 (or Rule 11) that applies.

As a member of the New Zealand Association of Counsellors, K also needs to consider the obligations set out in the NZAC's Code of Ethics. The NZAC Code of Ethics makes it clear that any information (including non-personal information) shared between K and J is confidential information and can only be shared with another person if one of the exceptions in the Code of Ethics applies.

In this case, J is not at immediate risk and has not consented to their information being shared, so none of exceptions in the Code of Ethics apply. K is not able to share any information that they hold about J with J's teacher.

The fact that K is employed by the school, rather than providing counselling services through a contracted service provider, does not change the fact that K cannot share information about J with J's teacher. The duty of confidentiality under the NZAC Code of Ethics is on K, not the school, as K is the person who has received and shared information with J as part of delivering the counselling services.

What if there were concerns about J's wellbeing or safety?

If there were concerns about J's wellbeing and safety, this would override the obligations of confidentiality set out in the Code of Ethics. In that case, K could

consider section 66C of the Oranga Tamariki Act to share relevant information about J with people at the school that were in a position to help J (so long as the purpose of sharing was for one of the purposes set out in section 66C) but would need to consider J's view that they did not want the information to be shared.

If there were serious concerns about J's health or safety, and none of the purposes under section 66C applied, K could share the information with appropriate people under IPP11 for the purposes of preventing or lessening a serious threat to J's health or safety, or the safety of others.

For more information about sharing information see Chapter 7: Sharing Information.

Collecting information

The education sector collects large volumes of personal information about learners. Privacy protective collection practices help ensure the privacy of your learners is protected and respected.

Schools, ECE services and contracted service providers have obligations and responsibilities under the Education and Training Act 2020, ECE regulations, and other child focused laws like the Children's Act 2014.

Collecting information from and about learners enables schools and ECE services to meet those obligations. Service providers collect learner information to identify, deliver and evaluate the effectiveness of the services they deliver.

In the digital age, the ways in which information can be collected is changing – it's not just paper forms and documents or conversations with others. Information can now be collected using various technologies, including:

- online enrolment and other online forms (e.g. google forms)
- learner and education management systems (e.g. student management systems)
- parent communication tools (e.g. Storypark, Educa, Hero, Seesaw, Skool Loop, KiwiSchools, SchoolAppsNz)
- devices in classrooms
- technology used to deliver education or services (e.g. google classroom)
- assessment and verification tools
- surveys
- CCTV

- photos and videos
- biometric technologies (e.g. fingerprint scanners).

When collecting information about learners, you need to get your privacy thinking right and ensure your collection practices are privacy protective. Not doing this can cause real harm that can impact learner wellbeing, engagement and achievement and undermine trust in the sector.

Good information collection practices:

- Make sure you are collecting only the information you need and that information collected is accurate and up to date.
- Enable the delivery of effective, learner specific services and supports that improve educational outcomes.
- Create transparency and build trust and confidence in how and why you collect learner information.

Due to a learner's age and ability, information will often be collected from other people such as their parents. Regardless of who the information is collected from, your primary focus should always be respecting and protecting the privacy of a learner's personal information and keeping their best interests front and centre when collecting their information.

Relevant information privacy principles

The Privacy Act 2020 (the Privacy Act) sets rules about what, when and how an education provider can collect personal information. Particular care needs to be taken when collecting personal information from or about learners.

The relevant information privacy principles (IPPs) for collecting personal information are:

Principle 1: Purpose for collection

An education provider can only collect personal information for a lawful purpose connected with a function or activity of the education provider and the collection of that information must be necessary for that purpose.

If your purpose for collecting personal information about the learner does not require the collection of identifying information, then you should not collect identifying information about the learner as part of that collection.

Principle 2: Source of personal information

When an education provider collects personal information, the information must be collected from the learner (unless an exception applies).

Exceptions include:

- the education provider believes, on reasonable grounds, that non-compliance will not prejudice the learner's interests
- complying with this requirement would prejudice the purposes of the collection
- the learner authorises the collection from someone else (if capable of doing so)
- the information is publicly available
- to prevent or lessen a serious threat to the life or health of the learner or any other individual
- the information will not be used in a form that could identify the learner
- the information will only be used for research or statistical purposes and will not be published in a form that could reasonably identify the learner
- that collecting from the learner is not reasonably practicable in the circumstances.

Principle 3: Collection of information from an individual

When collecting personal information directly from the learner you must take steps that are reasonable in the circumstances to inform them of:

- the fact that information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information
- the name and address of the education provider collecting and holding the information
- if the collection of information is required by law, the particular law under which the information is required, and whether the supply of information is voluntary or mandatory
- the consequences, if any, of not supplying the information
- the rights of access to and correction of the information supplied.

Principle 3A: Indirect collection (from 1 May 2026)

When collecting personal information from someone other than the learner you must take steps that are reasonable in the circumstances to inform the learner (or their parent where appropriate) of the following:

- the fact that information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information
- the name and address of the education provider collecting and holding the information
- if the collection of information is required by law, the particular law under which the information is required, and whether the supply of information is voluntary or mandatory
- the rights of access to and correction of the information supplied.

For more information about how to inform learners see: Chapter 8 Keeping Learners and Parents/Caregivers Informed.

You can only collect personal information about a learner indirectly if one of the exceptions in IPP 2 applies, or the collection is authorised by another law e.g. the Oranga Tamariki Act 1989 or the Family Violence Act 2018.

Principle 4: Manner of collection of personal information

An education provider can only collect personal information by lawful means and in a manner that is fair and does not intrude to an unreasonable extent upon the personal affairs of the learner – particularly in circumstances where personal information is being collected from learners directly.

What is a collection?

Under the Privacy Act a collection of personal information occurs when you take any step to seek or obtain the personal information. A collection of personal information does not include the receipt of unsolicited information.

In practice this means:

- When you take steps to seek (request) or obtain information about a learner, personal information you receive **will be a collection** and IPPs 1 – 4 will apply.
- When you receive information about a learner that you have not taken steps to seek or obtain, receipt of the personal information will be unsolicited and **will not be a collection** of information, but IPPs 5 – 13 will apply to the information you now hold about the learner.

Example – Complaints (collection)

When you receive a complaint that contains personal information, the personal information you receive will be a collection. While you haven't explicitly sought the information contained in the complaint, you will have processes in place that enable

a learner or their parents to make a complaint or raise a concern i.e. you have taken steps to obtain the information as part of your school or ECE service functions.

Example – Learner absence communications (collection)

When you receive a communication that a learner is absent (e.g. a text, email, or through a parent communication portal), the information will be a collection. As required by law, you will have processes in place to record a learner's attendance, including absences and the reasons for that absence i.e. you have taken steps to obtain the information.

Example - End of year progress report (not a collection)

The creation of end of year progress reports will not be a collection of personal information as they are created using personal information you already hold about a learner (e.g. progress and achievement information).

Example – Report from health care provider (unsolicited)

A school has received a copy of a psychologist's report about one of its learners. The report was commissioned privately by the learner's parents who authorised the disclosure of the report to the school. The learner is not receiving any learning support interventions from the school.

Is the receipt of the report unsolicited?

Yes. The school has not actively sought the report. In this case, IPPs 1 – 4 will not apply. However, as the school now holds the report and must ensure:

- that it is kept secure
- that it is only used or disclosed where an exception to IPP10 or 11 applies

- that the report is still accurate when it is used or shared
- that it is securely disposed of when it is no longer required to be retained.

For more information about retention and disposal of school records see: Chapter 12 Retaining and Disposing of Information.

Direct and indirect collection

There are two types of collection:

- **Direct collection:** When you collect personal information about a person directly from them (e.g. personal information about a learner collected directly from that learner, personal information about a learner's parent directly from that parent).

- **Indirect collection:** When you collect personal information from another person (e.g. personal information about a learner collected from someone else, including from the learner's parents).

It is important to understand what information you collect directly, and what information you collect indirectly, because different notification requirements apply.

For guidance on notification requirements see: Informing learners about collection of their information (IPP3 and IPP3A).

Do I need consent to collect a learner's personal information?

You do not need consent to collect a learner's personal information when you are collecting information directly from learners.

The Privacy Act 2020 uses the term authorisation rather than consent.

Authorisation (consent) is a consideration, however, when you:

- want to collect a learner's information from someone else (IPP2 exception)
- want to use or share a learner's personal information for a secondary purpose (IPP10 or 11 exception)
- deliver a service to a learner e.g. a learning support intervention.

For more information about the IPP10 authorisation exception to use a learner's personal information see Chapter 6: Using information.

For more information about the IPP11 authorisation exception to share a learner's personal information see Chapter 7: Sharing information.

Purpose of collection (IPP1)

You can only collect personal information if it is for a lawful purpose connected with the functions or activities of your organisation, **and** collection of that information is necessary for that purpose.

In practice this means you need to be clear about:

- the specific purpose you are collecting the information for
- how that purpose relates to your organisation's functions
- why and how the information is necessary for that purpose.

Have a clear purpose

Having a clear purpose for collecting information is critical.

A clear purpose will ensure you are only collecting information that you need, and that the information collected is used and shared appropriately. It also demonstrates to learners and their parents that the collection of information has been carefully considered with their privacy and best interest a key consideration.

Although it is not a requirement of the Privacy Act 2020, it is always good practice to consider whether your collection of personal information is in the learner's best interests. Broad purposes such as "delivering education services" or "wellbeing and safety of learners" can sometimes create ambiguity and confusion about how the information will actually be used. Broadly defined purposes also make it harder for learners (or their parents where appropriate) to make informed decisions about whether to provide the information in the first place (where they have the option to do so).

To help ensure your purpose is well-defined and appropriate, you first need to determine the problem the collection is intending to address, or the outcome the collection is trying to achieve. Identifying the underlying problem is not always obvious. Test your assumptions with other people within your organisation so you can be sure the purpose of your collection has been correctly identified and defined.

If you are collecting information directly from your learners, your purpose statements must in age-appropriate language.

Checklist for creating clear purpose statements

This checklist can be used to work through the process of developing a clear purpose for the collection of personal information.

- What is the problem you are trying to solve or the outcome you are trying to achieve?
- Is the problem or outcome connected to a lawful function of your organisation?
- Do you actually need personal information to solve your problem or achieve the intended outcome— or can you use aggregate or de-identified information to get the same result?
- What personal information do you need to solve your problem or achieve your intended outcome?

- How will the personal information be used to solve the problem or achieve your intended outcome?
- What personal information do you already hold and what are you missing to be able to solve your problem or achieve your intended outcome?

Examples of clear purpose statements

Our organisation provides several services to children and young people with learning disabilities. The information collected in our Needs Assessment form is used to identify which of our services will be most appropriate for your child and to allocate an appropriate practitioner.

It is important that we keep all our learners safe while they are attending the end of year school camp. We ask that you review your child's health information contained in the attached End of Year Camp Health Profile form and update it with any health or medical conditions that are missing, including any medication requirements your child may have while on camp. Your child's health information will be shared with and used by our camp managers to ensure they are aware of health and medical conditions your child may have and enable them to provide timely and appropriate assistance if required.

What does "necessary" mean?

Whether it is necessary to collect learner information for your specified purpose will depend on the circumstances.

You need to be able to show that:

- Collecting that personal information makes a clear, demonstrable contribution to achieving the specified purpose, and the information is relevant and not excessive or arbitrary.

- Collecting the personal information is a targeted, effective and accurate way to achieve that purpose: if it does not work, then it's unlikely it was necessary to collect the information in the first place.
- There is no less intrusive option that you could have reasonably and practically used in these circumstances to achieve the same result. If a less intrusive option is available and gets you to the same place, it is unlikely it was necessary to adopt the more intrusive option.
- The scope of information collection is also relevant to the degree of intrusion. The more information collected – and the more people affected – the more challenging it might be to show that collecting all that information is necessary to fulfil the purpose of collection. The degree of intrusion is also likely to depend on the privacy safeguards that are in place and whether they are effective.

Example – Collecting allergy information

An ECE service provides meals to its learners including morning and afternoon tea and a lunch meal. At the time of enrolment, the ECE service manager asks parents to provide information about any food allergies that their child may have.

The ECE service has to meet food safety and licencing obligations to ensure that all learners are safe while at the centre, including during mealtimes. In this case, it is necessary for the ECE service manager to collect information about any food allergies learners may have to ensure the safety and wellbeing of those learners during mealtimes.

Example – Collecting health information for school camp

A secondary school runs school camps for its learners. The deputy principal of the school obtains consent from learners' parents for their child to attend camp. As part of the consent process, parents are required to confirm information the school

already holds about their child's health or medical conditions and update that information if required.

The school has obligations to ensure the wellbeing and safety of the leaners while they are on camp. In this case, collecting information about any new health or medical conditions, including for example any daily medications that the learner may require while on the school camp, would be necessary to ensure the school camp managers are aware of all possible health risks and medication requirements and are able to respond appropriately should a medical event occur.

Example – Collecting unnecessary information to determine eligibility

A non-government organisation (NGO) provides learning support services to schools and ECE services. When a learner is referred to the NGO from a school or ECE service, relevant information about the learner is provided in the referral form including the learners name, age, address, name and contact details for the parents, and the reason for the referral. The NGO administrator enters the referral information into the case management system then allocates a practitioner for a service eligibility assessment.

The practitioner contacts the learner's parents and asks them to complete a service eligibility form. The NGO's service eligibility form requires parent to provide information about the learner's siblings.

Given the eligibility assessment is in relation to the learner specifically, it would unlikely be considered necessary for the NGO to collect information about the learner's siblings for the purposes of assessing whether a learner is eligible for their services.

Example – Collecting unnecessary enrolment information

An education provider's enrolment form requires parents to provide information about their occupation. Each section of the enrolment form must be completed before it can be submitted to the school.

In this case, information about a parent's occupation is not likely to be necessary for the specific purpose of assessing and confirming a learner's enrolment with the education provider.

Parent occupation information may be necessary for other lawful purposes, but these secondary purposes should be clearly documented in the enrolment form so that the parents are fully informed about how that information will be used.

Collection should be from the individual (IPP2)

When you collect information about a learner you are required to collect it directly from them, unless an exception to IPP2 applies.

The requirement to collect information directly from a learner ensures they are aware of the collection of their information, the reasons why their information is being collected, and have the opportunity to consider whether they want to provide the information or not (if the collection is optional).

However, the reality is that education providers collect a significant amount of personal information about learners from parents (or someone else). There are some exceptions to the requirement to collect personal information from the learner that are relevant to the education sector, including:

- the education provider believes, on reasonable grounds, that non-compliance will not prejudice the learner's interests
- compliance would prejudice the purposes of the collection

- the learner authorises to the collection from someone else (if capable of doing so)
- the information is publicly available
- to prevent or lessen a serious threat to the life or health of the learner or any other individual
- the information will not be used in a form that could identify the learner
- the information will only be used for research or statistical purposes and will not be published in a form that could reasonably identify the learner
- that collecting from the learner is not reasonably practicable in the circumstances.

If, in the circumstances, you reasonably believe an IPP 2 exception applies:

- you can collect the information about the learner from someone else
  and
- you will need to comply with the IPP3A notification requirements (from 1 May 2026).

For more information about IPP3A see our guidance: Office of the Privacy Commissioner | IPP3A: notification requirements for indirect collection of personal information.

Not reasonably practicable exception

It may not always be reasonably practicable to collect information directly from your learners. This could be for a number of factors, including:

- the age of the learner
- the learner's ability to:
  - understand why the information is being collected
  - provide the information (e.g. write or complete an online form)

- provide accurate information about themselves (e.g. health or medical conditions).

For example, due to their age and ability, learners may not know and might not be able to provide all the information required in an enrolment form – in this case, it isn't reasonably practicable for the learner to provide the information necessary for the purposes of enrolment.

For schools or service providers working with older learners, you will need to consider whether, in the circumstances, you should be collecting personal information directly from those learners. This will be particularly important when you are collecting sensitive information like health, gender identity, or wellbeing and safety information.

Inconvenience, cost, or administrative burden related to collection of the information are factors to consider under this exception, but it is always best practice to collect directly from a learner when you can.

Non-compliance won't prejudice the interests of a learner exception

In some cases, collecting personal information about a learner from a parent or someone else won't prejudice their interests.

In practice, this means that the learner wouldn't suffer any detriment as a result of their information being collected from another person. What is detrimental will often depend on the circumstances of the learner e.g. age and ability.

For example, due to their age and ability, a learner's interests wouldn't be prejudiced by collecting health information (e.g. information about food allergies). It would be in the learner's interests for necessary and accurate health information to be provided.

Before relying on these two exceptions, you need to consider whether you should collect information (in full or in part) directly from the learner.

It is a good idea to document your reasons for using these two exceptions, including why you believed that it was not reasonably practicable to collect the information directly from the learner or why an indirect collection of information about the learner wouldn't prejudice their interests.

Authorisation (consent) to collect from another person exception

You can collect a learner's personal information from another person when the learner has provided authorisation (consent) for you to do so.

You will need to ensure that the learner is capable of providing authorisation before you rely on this exception. You must also ensure that you only collect the information from the person the learner provided authorisation for.

When collecting information from that person, you should let them know that the learner has authorised the collection and provide evidence of that authorisation.

Informing learners (IPP3 and 3A)

Being transparent about why and how you collect (and then use and share) a learner's personal information is a requirement of the Privacy Act. Being transparent also helps you to build trust and confidence with your learners (and their parents) in the way you manage their personal information.

Informing learners about collecting their information is not a 'one and done' thing. Each time you collect their personal information you need to determine how to inform them of the collection, and what that communication should look like.

If it has been a while since you last collected information for a specific purpose (e.g. an annual survey), it is a good idea to remind your learners about the collection. If you have made a significant change to an existing collection, you should also tell your learners about those changes.

IPP3 Notification for direct collection

When you collect information directly from the learner you are required to tell them about the collection unless an IPP 3 exception applies.

IPP3A Notification for indirect collection (applicable from 1 May 2026)

From 1 May 2026, when you collect information indirectly (e.g. from a parent, or another person or organisation), you will be required to let the learner (or their parent where appropriate) know about the collection unless an IPP3A exception applies.

For more information about how to inform learners see Chapter 8: Keeping Learners and Parents/Caregivers informed.

For more information about IPP 3A see our guidance: Office of the Privacy Commissioner | IPP3A: notification requirements for indirect collection of personal information.

Collection methods must be lawful, fair and not intrusive (IPP4)

The way you collect personal information matters, especially when you are collecting information from learners themselves.

You must take particular care about how you collect information from your learners. It may not be appropriate to collect information from learners in the same way you collect information from their parents or other people.

When collecting a learner's information, you must ensure that the means by which you use to collect their information is:

- lawful
- fair
- not unreasonably intrusive to a learner's personal affairs.

What is fair and not unreasonably intrusive will depend on the circumstances of the learner concerned, such as age or ability, the sensitivity of the information, and the purpose for which the information is being collected. At all times, the best interests of the learner should be a consideration in your decision making.

Fairness considerations

If learners don't understand the reasons why you are collecting their information and how you are going to use it, the means of collection could be considered unfair.

If you have decided not to inform your learners (or their parents where appropriate) about the collection, you will need to demonstrate that one of the exceptions of Information Privacy Principle (IPP) 3 (or IPP3A after 1 May 2026) apply in the circumstances.

When you are collecting information directly from your learners (e.g. through an in-class learner wellbeing survey or a programme evaluation process) you need to ensure that you are informing them in a way that they will understand. This is the case even if you have informed the learner's parents. Take the time to talk your learner through the collection and ask them questions to determine their level of understanding.

You should also consider whether to it would be helpful to develop different communication content and delivery methods for different age categories of learners as well as their parents.

Intrusiveness considerations

If you collect information from or about learners for purposes that are outside the scope of your lawful functions or activities, or you collect more information that is necessary to achieve your lawful functions and activities, there is a risk the collection

of that information could intrude on the personal affairs of your learners or other people such as the learner's parents or family members.

Understanding the circumstances about a learner's home life may often be relevant to understanding the risk of harm to a learner and responding appropriately to suspected or actual child abuse or neglect. Such circumstances could include:

- where a learner has indicated (directly or indirectly) that they need help
- where you have observed a change in behaviour in the classroom or during the delivery of an education support service (e.g. a usually vibrant learner has become withdrawn, or for school counsellors where a learner has disclosed family issues through a counselling session)
- where you have been advised by another person or agency that the learner may be experiencing difficulties and may be at risk of abuse or neglect (e.g. via the School Alerts Programme for learners subject to family harm).

However, there may be other ways to collect this information from a learner to ensure their needs are met appropriately (e.g. from the learner or their parents directly, from other people that know or could help the learner) that don't involve large scale collections of information from multiple learners for whom there may be no wellbeing or safety concerns.

Example – Learner wellbeing surveys

A primary school wants to implement a weekly learner wellbeing at school survey for learners. The purpose of the survey to ask the learner questions about how they are feeling that day about a range of topics enabling the school to identify students that may need additional wellbeing support. The survey will also provide the learner the option to "ask for help" if they need it.

The school leadership team is working through the process of what questions to include in the survey. While the majority of the questions relate to the school environment, the leadership team has also included questions about the learner's home life such as:

- the size of their house
- whether they have a place to do homework
- whether their house is warm
- whether the family has enough money for necessities
- whether they have siblings that attend the school
- alcohol or drug use
- gang affiliations.

A member of the leadership team has raised concerns that the homelife questions could be unreasonably intrusive and breach IPP4.

Depending on the circumstances, collecting information about a learner's home life (such as those listed above) may be considered an intrusion into the personal affairs of the learners and other people living in the home. The school will need to be able to justify it has a lawful purpose for collecting this information, and that the information about the learner's home life is necessary for that purpose. Without such a justification, the collection of information about a learner's homelife as part of a whole of school survey will be considered an intrusion into a learner's personal affairs.

There is also a fairness issue connected to the collection of information about a learner's home life. Depending on the age of the learner, they may not understand why they are being asked questions about their home life or the meaning of the questions that are being asked. As such, a learner could feel pressured to provide an answer. A learner may be annoyed at their parent or caregiver for saying no to the

purchase of a certain item, for example, which may then lead them to answer questions in a different way.

When designing questions, the school will also need to think about whose personal information they are collecting. Questions about a learner's homelife may include the collection of information about family members. The school needs to consider how IPP2 would apply to this collection and who needs to be notified under IPPs 3 and 3A.

Example – CCTV in bathrooms/locker rooms

A High School has installed CCTV cameras in all bathrooms and locker rooms to combat an increase in smoking, vaping and bullying incidents. The school has completed a Privacy Impact Assessment, has communicated to all its learners and their parents that CCTV has been installed and why, and has clear signage at the entrance to all locations that the CCTV cameras are present and recording.

A learner has complained to the school's privacy officer that the CCTV cameras in the bathrooms are positioned in a way that captures the toilets in the bathrooms, and showers in the locker rooms. The learner believes that the position of the CCTV cameras is breaching their privacy by collecting information in a way that unreasonable intrudes on their personal affairs – going to the toilet and taking a shower.

In this case, the CCTV cameras are collecting information that relates to the personal affairs of the learner (toileting and showering). While the school may have a lawful purpose for installing the cameras (safety of learners, and identifying misconduct), the collection of information that includes intimate activities would unreasonably intrude on the personal affairs of the learners. The school should reposition the CCTV cameras to ensure they focus away from personal affairs such as toileting and showering.

For more information on CCTV and school bathrooms see: Office of the Privacy Commissioner | CCTV and school bathrooms.

Example – Video recording of a learner support session

A speech language therapist works for an organisation that provides speech language therapy to children and young people. The organisation often receives referrals from local schools and ECE services for learners who have learning support needs. The speech language therapist works with a number of these learners and their families virtually as they can't attend the sessions in person.

After getting authorisation (consent) from the learner and their parents, the speech language therapist records some of the therapy sessions. The purpose of recording the sessions to enable them to review the progress of the learner over time, identify where additional therapy protocols may be useful, and show the learner and their parents the progressbeing made.

Before the recording of any sessions, the speech language therapist asks the learner and their parents to check whether there is anything in the background that they may not want captured in the recording. Where it is appropriate to do so and doesn't impact the effectiveness of the therapy, the learner is advised that they can blur their background if they want to.

In the circumstances, the collection of personal information through recording the virtual therapy session would not unreasonably intrude on the personal affairs of the learner or their parents as the learner and their parents have been informed:

- that the session is being recorded and why
- they can ask for the recording to stop at anytime
- they can check the background to check that nothing personal and irrelevant to the therapy session will be in the recording
- where appropriate, they can blur the background.

Example – Recording an interview with a learner

The principal of a secondary school is preparing to interview a learner as part of a disciplinary process. The learner's parents will be present for the interview. The principal wants to audio record the interview to ensure they create an accurate record of the interview.

Can the principal record the interview without the learner's knowledge?

The principal should not record the interview without the learner or their parent's knowledge. Covert or secret recording is intrinsically intrusive. In a disciplinary interview situation, the principal should explain to the learner and their parents why they want to record the interview, how the recording will be used, who it may be shared with, and the learner's right to request access to and correction of the recording. It would also be best practice to make the learner and their parents aware that the recording will be deleted after the disciplinary process is completed as it is required to be retained by the school as a school record.

Just because you can, doesn't always mean you should

When collecting personal information about learners, it is always best practice to consider any ethical issues that the collection may raise. Taking a moment to consider any ethical issues helps to ensure the best interests of the learner, or groups or learners, are forefront of your collection practices.

The Data Protection and Use Policy (DPUP) is a useful tool that sets out expectations for respectful, trustworthy and transparent collection and use of personal information. DPUP is made up of a set of principles and guidelines that focus on values, behaviours and relationships.

DPUP complements the Privacy Act and other legislation governing the collection, use and sharing of personal information, and can help you work through the "*I can, but should I*?" question when you are collecting personal information about learners.

For more information about DPUP see: Data Protection and Use Policy (DPUP) | NZ Digital government.

Collecting information in practice

This section provides some additional examples of collecting learners' personal information in the education sector.

Conversations and Meetings

We often don't realise how much personal information we collect about a learner through our everyday conversations and meetings with other people.

Not all information shared with you during conversations or meetings will be considered a collection of personal information under the Privacy Act.

For example:

- When, during a conversation or meeting, you directly seek (request) information about a learner, the personal information you receive **will be a collection.**
- When you obtain information verbally rather than through an established written process connected to your organisation's function (e.g. a complaints process, or a general enquiry email address for enrolments), the personal information you receive **will likely be a collection.**

- When, during a conversation or meeting, you receive information about a learner that you have not taken steps to seek or obtain (i.e. there is not a process in place for that information to be provided), the receipt of the personal information will be unsolicited and **will not be a collection** of information.

Collection Examples

Where personal information is **sought** (requested):

- seeking information from a parent about any challenges their child may be experiencing at home which is impacting their learning
- information shared with you in response to you requesting information about a specific learner
- a principal receiving information they have requested about a learner who is wanting to enrol at their school
- interviewing people as part of an investigation or disciplinary process.

Where personal information is **obtained**:

- a parent talking to you about their child and challenges they are experiencing at home which may impact their learning
- an email from a child welfare and protection agency proactively sharing information about a learner who is receiving care and protection services
- a meeting with a parent where the parent shares information about their concerns of bullying by other learners
- information shared with you at a staff meeting (in person or online) about a learner.

When you collect (request or obtain) information from another person, it is important to remember:

- that the person sharing the information will need to ensure they have an appropriate legal authority to share the information with you (see Chapter 7: Sharing Information)
- to collect information in a way is privacy protective – make sure other people can't overhear your conversation
- when you are collecting personal information directly from the learner (or their parent where appropriate), the notification requirements of IPP 3 will apply
- when you are collecting personal information about learners from other people, it will be an indirect collection of personal information and the notification requirements under IPP 3A will apply (from 1 May 2026)
- to manage information collected or obtained through conversations and meetings the same way you would if they information was collected or obtained through an email, a letter, or an online form.

Verbal Conversations

Verbal conversations can be a quick and effective way to help resolve a problem or seek ideas about how to manage challenges with a particular learner.

However, before requesting personal information in a conversation with another person about a learner, you should think about the following:

- Do you really need personal information about the learner, or can you resolve your problem with more general information?
- If you do need personal information what personal information might you need from the other person?
- If you have to identify the learner, what is the minimum amount of information that you need to share to enable the other party to conversation to provide the requested information about the learner?

- Where do you plan to have the conversation – can other people overhear your conversation?
- Do you have the ability to document the information you are provided – you may not document the information accurately if you make notes later
- Is now the right time to have the conversation with the other person – would it be better to set up a meeting to discuss the issue?

When you collect personal information verbally from another person, it is always best practice to securely document the information you received including who you received it from and when, as soon as you can.

Information collected verbally is subject to the Official Information Act 1982 and the Privacy Act 2020.

Internal meetings

Staff meetings are a regular occurrence – in most cases there isn't a day where you aren't involved a meeting of some kind. Staff meetings are important as they provide a safe and collaborative environment for staff to discuss their thoughts, ideas and concerns on a variety of matters.

Meetings may involve a number of different staff and involve discussions about different learners. As a general rule, personal information about learners should not be requested or shared in general staff meetings – not everyone in the meeting will need to know that information about the learner. Where possible matters about learners should be discussed in a non-identifiable way.

Where the purpose of the meeting is to discuss a learner, or group of learners, only staff members that need to know or can help with resolving the issue should be present. Make sure you have a clear purpose for the meeting, and only collect personal information from meeting participants that you need.Use the checklist above to help you create a clear purpose for your meeting.

Invites sent to meeting participants should not contain personal information about the learner other what is necessary for people to decide to attend and prepare. Where meetings are held in an online environment, avoid putting information about learners in the chat function, or using the meeting transcription functionality.

When you collect or obtain personal information from another person in a meeting, it is always best practice to record the information you receive in a secure location, including who you received it from and when, as soon as you can.

If your organisation is subject to the Official Information Act 1981, information collected verbally is subject to both the Official Information Act 1981 and the Privacy Act 2020.

Be mindful when taking meeting minutes. It may not be appropriate to record personal information, particularly that of a more sensitive nature, in meeting minutes, especially if the meeting minutes are distributed. It may be more appropriate to record the information in a location where access to the information is adequately protected from unauthorised access, use or sharing.

Also be aware of AI online meeting assistance or transcription functionality. While such functionality may appear useful or save time taking minutes, it can create significant privacy risks for learners and meeting participants.

For more detailed information about using digital tools, including AI, see Chapter 16: Technology in Education.

Multi-agency meetings

A multi-agency meeting is a meeting where different agencies and organisations come together for a common purpose. These meetings can be one-off events or occur regularly.

To provide services and deliver effective outcomes, you often need to collect information (both verbally and in written form) about learners from other agencies or organisations. Collecting and sharing information at multi-agency meetings enable

those attending to understand and quantify the extent of a problem, providing relevant information about the learner, and then identify appropriate and effective supports, interventions, and services.

If you seek (request) or obtain personal information about a learner during a multi-agency meeting, this will be a collection of information.

For more detailed information about requesting and sharing personal information at multi-agency meetings see: Sharing information at multi-agency meetings.

Surveys

Surveys can sometimes be a good tool to collect information about a specific issue from a large number of learners. Surveys are also a useful way for learners to contribute to decision-making or provide feedback on a proposal or initiative that impacts them.

However, the use of surveys can create additional privacy risks that you need to consider. Information collected through a survey can include personal information, for example – a learner's thoughts and opinions about how something may impact them personally, or personal information about other learners or staff. Surveys can also collect information that might unreasonably intrude on a learner's personal life (for example, learner wellbeing surveys).

Therefore, the privacy of learners must be a primary consideration when using surveys to collect personal information.

Things to think about when designing a survey

You must have a clear purpose for your survey. Use the creating a clear purpose checklist above to help you determine your purpose and whether you need to collect personal information through your survey.

To ensure your survey is protective of learner's privacy you should also consider:

- whether there are other ways, including existing processes and communication channels, to collect the information you need
- whether learners could inadvertently provide personal information even though you haven't asked for it and do you have process for managing that information
- whether the method of collection and the information requested could identify the learner
- whether you are required to inform the learners (or their parents where appropriate) about the survey and what that you need to tell them
- whether you can actually do anything with the information you receive
- where will you store the survey results and how you will protect them from unauthorised use and sharing
- whether you plan on combining the survey information with other information you hold about the learner
- how long you may need to keep the survey information.

Use of survey tools

There are a number of survey tools that education providers may use. When using a survey tool, typically a third-party provider collects the information on your behalf and then provides you with the survey results.

It's important to remember that you are responsible for ensuring that your collection of information complies with the Privacy Act, whether you are collecting personal information using a survey directly or using the services of a third-party provider. You still need to ensure that your collection of learners' information has a clear purpose and the information being collected is necessary. Any survey tool is just the mechanism by which you collect the information.

You should also inform your learners (and their parents where appropriate) that you are using a third-party survey tool and provide a link to the third-party provider's

privacy statement, as well as your own. This way, learners (and their parents where appropriate) can make informed decisions about the use of the survey tool.

Before using any survey tool, you also need to consider:

- how personal information is kept secure
- how long the third-party provider may retain the information
- whether the third-party provider sells or uses the information for its own purposes or for other commercial purposes
- whether the third-party provider uses AI to process the information being collected.

Free versions of survey tools often come with more privacy risks, so extra care should be taken before using free survey tools to collect a learner's personal information.

For more detailed information about using digital tools, including AI, see Chapter 16: Technology in Education.

Consider completing a Privacy Impact Assessment for your proposed survey

A privacy impact assessment is a tool you can use to assess the potential privacy impacts of a new project (e.g. a new collection of personal information, or the use of a third-party survey tool to collect personal information) or changes to an existing project or system.

Undertaking a privacy impact assessment is a good way to assess your survey (or any other collection of personal information) against all the information privacy principles, not just those that relate to the collection of personal information. Completing a privacy impact assessment demonstrates to learners (or their parents) that you have carefully considered the collection and taken measures to identify and mitigate any privacy risks.

For more information about how to complete a privacy impact assessment see our guidance: Office of the Privacy Commissioner | Privacy Impact Assessments.

Enrolment forms

Enrolment forms are used to collect information about a learner to support an education provider to make decisions about enrolling the learner in an ECE service, school or education-related service.

Information necessary for enrolling a learner

Only information necessary for the **purposes of enrolling a learner** should be collected through your enrolment form.

What information is necessary will depend on your circumstances. Some education providers may require specific information to assess and complete an enrolment, for example:

- An ECE service may require specific information to be provided to ensure it meets its funding and licencing requirements.
- A school or early learning service that provides lunches may require specific information about a learner's food related medical conditions.
- A private school may require specific information to enable relevant enrolment assessments to be undertaken.
- A specialist school may require specific information to determine whether the learner is eligible and what their needs are.
- A school may require specific information from a learner where the Ministry of Education has directed an enrolment under the Education and Training Act 2020.
- A service provider providing speech language therapy may require specific health information about the learner to determine whether the learner is eligible for enrolment and services provided.

Ministry of Education information requirements

The Ministry of Education requires schools and ECE services to collect certain information about a learner as part of the enrolment process. Schools and ECE services are required to collect this information from learners and share it with the Ministry.

For more information about the Ministry of Education information requirements see:

Schools: School Enrolment Form Guidelines | Education Counts

ECE services: Chapter 14: Collection of information - Ministry of Education and Early Learning Information and Privacy.

Informing learners and their parents

Every enrolment form should include a privacy statement informing learners (and their parents) about why the information is being collected, what the information will be used for, and what information may be shared with other organisations. This privacy statement should be specific to the information being collected through the enrolment form. Learners and their parents should also be informed about how they can access and correct the enrolment information.

For guidance on what to include in your enrolment form privacy statement see: Chapter 8: Keeping Learners and their parents informed.

Collection of information to verify identity or eligibility

If you are required to verify identity or eligibility to complete a learner's enrolment (for example, a learner's age or citizenship status) you may need to collect identity documents to complete the verification process.

Where you collect identity documentation (for example, a copy of a birth certificate or passport) for verification purposes that information should only be used for the specific purpose of verification. Once the verification process is complete, the identity documentation may or may not need to be securely retained.

For more information on retention and deletion of personal information see Chapter 12: Retaining and Deleting information.

Extra care should be taken when collecting identity documentation. Some of the larger privacy breaches have involved identity documentation held by organisations that did not securely delete these documents after verifying an individual's identity or eligibility for services.

Review your enrolment forms

It is good practice to review your enrolment forms to ensure they remain up to date and fit for purpose, especially your enrolment form privacy statements.

For example, legislative requirements may have changed, or you may disclose personal information to new agencies or organisations. These changes to the way you collect, use and share a learner's enrolment information need to be communicated to learners (and their parents).

An easy way to make sure these reviews happen, is to add the review to your privacy officers work plan.

Photography and Filming

Many schools and ECE services utilise social media and other online platforms to celebrate their learners' achievements with parents and the broader school or ECE community. Technology such as videoconferencing and online classrooms also assists education providers to provide services to learners that may not be able to attend class or sessions in person.

While there are many benefits to taking photos or videos there are also risks. When you take photos or videos of learners you will be collecting personal information about them. It is important to be aware of the risks and do what is necessary to protect your learner's privacy and keep them safe.

For more information about the collection, use and sharing of images of children and young people see our Photography and Filming guidance: Office of the Privacy Commissioner | Children and young people: photography and filming guidance

For more general information about the use of CCTV see our CCTV guidance: Office of the Privacy Commissioner | CCTV.

For information about responding to requests for CCTV footage see our guidance: Office of the Privacy Commissioner | Responding to access requests for CCTV footage and also Chapter 13: Managing Requests for Information.

Learner wellbeing and safety

There may be times when you need to collect information about the wellbeing or safety of a learner. It is always best practice to collect this information directly from the learner (or their parents where appropriate). However, this may not always be possible or appropriate.

The Oranga Tamariki Act 1989 and the Family Violence Act 2018 enable you to request information about learners in certain circumstances:

- The Oranga Tamariki Act permits specified agencies and organisations request information about learners for wellbeing and safety purposes.
- The Family Violence Act permits specified agencies and organisation to request information about learners for purposes of protecting them from family violence.

For more detailed information about requesting information using the Oranga Tamariki Act and the Family Violence Act see:

- Information Sharing: Office of the Privacy Commissioner | Sharing information to protect the wellbeing and safety of children and young people.
- Chapter 7: Sharing Information

- Oranga Tamariki Act Guidance for sharing information | Oranga Tamariki — Ministry for Children.
- Family Violence Act Sharing-Information-Safely.pdf

Using information

Education providers use personal information about learners every day. A learner's information should be used appropriately to support their education journey.

Using the personal information that you hold appropriately is essential to:

- build learner and parent trust and confidence in how you use personal information that you collect and hold
- delivering education services that enable and support attendance and achievement
- identifying and providing effective learning support interventions in a timely manner
- supporting a learner's wellbeing and safety.

Relevant information privacy principles

The Privacy Act 2020 provides clear rules about how personal information that you hold about learners (and other individuals) can be used, and the purposes for which you can use it.

The relevant information privacy principles (IPPs) for using personal information are:

Principle 10: Limits on use of personal information

An education provider that holds personal information that was obtained in connection with one purpose may not use that information for any other purpose unless it believes, on reasonable grounds, that an exception applies.

Principle 8: Accuracy of personal information to be checked before use or disclosure

An education provider that holds personal information must not use or disclose that information without taking steps that are reasonable, in the circumstances, to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

When you want to use information that you hold for learner wellbeing or safety purposes you should consider section 66C of the Oranga Tamariki Act before deciding whether an IPP10 exception applies.

When you want to use information that you hold about a victim or perpetrator of family violence you should consider section 20 of the Family Violence Act before deciding whether an IPP10 exception applies.

See: Using information for wellbeing, safety or family violence purposes section.

Using information for the purpose it was collected

IPP10 requires you to use personal information you hold about your learners for the purposes for which it was originally collected (unless an exception applies).

When you are collecting information from or about your learners, it is important to be clear about why you are collecting it and what you are going to use the information for. This makes it easier to make sure you are only using a learner's personal information for the purposes for which it was collected.

For more information about collecting learners' personal information, including purpose of collection, see: Chapter 5: Collecting Information.

Example – Following up on absence from school

A school collects attendance information of its learners and maintains an attendance register. The school also holds contact information about parents that is collected through the enrolment process.

A teacher notices a pattern of absence of a learner and wants to contact the parents to talk to them about their child's absences from school.

Can the teacher use the attendance and parent contact information for this purpose?

Yes. Attendance information is collected for a number of purposes, one of which is to make sure learners are attending school and to identify learners whose absence may be impacting their learning progress. A teacher using the attendance information to identify absence trends is one of the purposes for which the attendance information was collected.

Parent contact information is collected so that the school can communicate with the parents about their child, including matters that may be impacting their child's learning. Contacting the parents about their child's absence from school is a purpose for which the parent contact information was originally collected.

Example – Reporting on a learner's progress and achievement

During the year, learners submit work for assessment. The teacher marks the assessments and enters the results into the student management system. The teacher wants to use this information to complete end of year progress reports for their learners.

Can the teacher use the assessment information?

Yes. The assessment information is collected to measure a learner's progress and achievement. Using the assessment information to prepare an end of year progress and assessment report is one of the purposes for which the information was collected.

Example – Health information collected for the purposes of school camp

A secondary school runs a school camp for its learners. As part of the consent process information about new health and medical conditions is collected. Parents are informed that this information will be used for the purposes of ensuring designated school camp managers are aware of all possible health risks and medication requirements and are able to respond appropriately should a medical event occur.

Later during the year, a learning support coordinator, who was one of the school camp managers, is developing a learning support needs assessment for a learner. They are aware of the health information provided by the learner's parents for the purposes of attending the school camp in the needs assessment.

Can the learning support coordinator use the information?

No. The health and medical information were not collected for learning support purposes. The intended use of the health and medical information is a secondary use of the information.

For more information about health and learning support information see Chapter 9: Health and Learning Support information.

Example – Secondary use of assessment information

A secondary school has a competitive first XV rugby team that is coached and managed by a couple of teachers. The coach and manager determine the membership of the team through pre-season trials. The quality of the learners trialling for the first XV is high and as a result a number of excellent players will likely miss out on selection. To help determine the final team player, the coach and manager want to consider the academic achievement of the learners as part of the selection process.

Can the learner's achievement information be used for this purpose?

No. While the coach and manager may have access to this information, using that information for the purposes of selecting a first XV rugby team is not one of the purposes for which the achievement information was originally collected. The coach and manager can't use this information unless one of the IPP10 exceptions apply.

IPP10 exceptions

IPP10 contains a number of exceptions that enable the use of personal information for purposes other than the original purpose the information was collected for (secondary purposes).

The exceptions that commonly apply within the education sector include:

- The purpose for using the information is directly related to one of the purposes for which the information was obtained.
- The learner (or their parent where appropriate) has authorised the other use of their information.
- The information is being used in a way that does not identify the learner.
- Using the information is necessary to prevent or lessen a serious threat to the learner's or another person's life or health, or public health and safety.
- Using the information about the learner is necessary to maintain the law (e.g. enrolment fraud investigations).

What do you need to consider when applying an IPP10 exception?

Deciding whether an IPP10 exception applies will be a judgement call and will depend on the circumstances. To help you decide whether an IPP10 exception applies in the circumstances you should consider:

- Are there reasonable grounds to believe that the exception applies in the circumstances?
- Is use of the information necessary to achieve the purpose of the exception?
- Is the information you are intending to share accurate, up to date, complete, relevant and not misleading?

The following sections look at these considerations in more detail.

You must believe on reasonable grounds that an exception applies

To rely on an IPP10 exception, you **must**:

- believe that the exception applies at the time you are wanting to use the information

  and
- your belief must be reasonably held.

This means you need to consider whether the exception applies before you use the information for a secondary purpose, and you must have properly considered all the relevant information in the circumstances.

Whether there is a reasonable basis will depend on what you know at the time you want or need to use the learner's information.

If you do not have enough information to decide that the IPP10 exception applies you shouldn't use the learner's personal information (unless section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act applies).

Some exceptions require you to consider necessity

The IPP10 exceptions for preventing or lessening a serious threat and maintenance of the law also require you to consider whether using the information is necessary in those specific circumstances.

Whether the use of the information for these specific exceptions is necessary is a relatively low threshold - is the use of the information needed or required in the circumstances, or required for a given situation?

To help decide whether the use of information is necessary you should consider whether not using the information could, in the circumstances:

- increase the likelihood of the serious threat occurring (e.g. an infectious disease spreading through the school or ECE service)
  or
- compromise your ability to maintain the law (e.g. investigate suspected enrolment fraud).

Is the information accurate, up to date, relevant, complete and not misleading?

IPP8 requires that you take reasonable steps to make sure a learner's personal information is accurate, up to date, relevant, complete and not misleading before you use it.

Using inaccurate, out of date, irrelevant, incomplete or misleading information can result in prejudicial information about the learner being used to make decisions about them. This can have significant short- and long-term impacts for the learner.

Take the time to check the information is accurate, up to date, relevant, complete and not misleading before you use it.

Make sure you are using the latest versions of documents or learner records before you use them.

For more information about accuracy requirements see Chapter 10: Accuracy of Information.

Can I use sensitive information?

The Privacy Act does not define or provide rules around the use of sensitive information. However, in practice, special care should be taken when using intimate or particularly sensitive personal information about a learner. Sensitive information is information that has some real significance to the learner, is revealing, or generally relates to matters they might wish to keep private.

However, there may be situations where using sensitive information is necessary – for example, when there is a serious threat to a learner's life or health. The relative sensitivity of the information, and whether it is in the best interests of the child or young person, will be an important consideration when thinking about using sensitive information.

For more information about sensitive personal information and the Privacy Act see: Working with sensitive personal information.

Do I need consent to use information under an IPP 10 Exception?

One of the IPP10 exceptions is the authorisation (consent) of the individual. This means that you can obtain the authorisation (consent) of the learner (or their parents where appropriate) to use their personal information for a secondary purpose.

When relying on another IPP10 exception, you **do not** need the consent of the learner (or their parent where appropriate) to use their information.

For more information about obtaining consent to use a learner's personal information see: Authorisation (consent) in practice.

Using IPP10 exceptions in practice

This section provides some common examples of using IPP10 exceptions in practice.

Authorisation (consent) exception

IPP10 provides an exception where personal information about a learner can be used for a different purpose to that it was initially collected for if the learner (or their parent where appropriate) provides authorisation (consent).

You will need to consider whether the learner is old enough to be able to authorise the intended use of their information. Where the learner is younger, or not sufficiently able to understand, then you should obtain authorisation from the learner's parents.

For a learner (or parent where appropriate) to make an informed decision about authorising the use their personal information for a different purpose, you will need to ensure that the learner (or their parents where appropriate) has sufficient information to make an informed decision.

Obtaining authorisation can be done through:

- a **consent form** where a learner (or their parent where appropriate) can explicitly authorise the intended use
  or
- an **opt out form** where information about a learner will be used for a specified purpose unless the learner (or their parents where appropriate) opts out.

You should attach the collection privacy statement to the authorisation (consent) or opt out form. The privacy statement will provide the learner (or their parents where appropriate) with the information they need to make an informed decision to authorise the intended use of the information. You should also provide a link to your privacy policy in your authorisation or opt out form so that learners (or their parents where appropriate) can have confidence in how you collect, use, share and protect personal information more generally.

Detailed guidance on how to inform learners and their parents can be found in Chapter 8: Keeping Learners and parents informed.

Authorisation is not a 'one and done' thing. Where authorisation has been provided, learners (or their parent where appropriate) should be able to withdraw that authorisation at any time. Also, if it has been some time since the learner (or their parent) provided authorisation for their information to be used you should check whether they are still comfortable with the information being used for that purpose.

When a learner (or their parent where appropriate) withdraws authorisation

A learner (or their parent or legal guardian where appropriate) can withdraw authorisation they have **previously provided** for their information to be used for specified purposes.

For example, learners (or their parent where appropriate) may withdraw authorisation for their images to be used for advertising purposes.

When a previously provided authorisation is withdrawn, you must stop using their information for the purpose to which the authorisation applied.

When you are relying on one of the other IPP 10 exceptions, section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act, to use a learner's personal information for a secondary purpose, the learner (or their parents where appropriate) will not be able to withdraw their authorisation (consent). This is because their authorisation was not the basis relied on for using their information.

Directly related purpose exception

IPP10 provides an exception where personal information about a learner can be used for a directly related purpose to that for which it was originally collected.

In practice, this means that there must be a direct relationship between the purpose for which the information was originally obtained and the purpose for which you now want to use the information.

When determining whether the secondary use of a learner's information is directly related to the original purpose you collected it for you should consider:

- the original purpose of collection
- the relationship between the original and secondary purpose
- whether the learner (or their parent where appropriate) would reasonably expect the original and secondary purposes to be directly related to each

other (i.e. what were they informed when the information was originally collected)

- what information you need to use to achieve the secondary purpose.

Example – Programme or service evaluation (directly related)

An education provider ran a learning support initiative that provided learners with additional learning supports. A number of learners participated in the initiative, and they were informed at the time of signing up to participate that the education provider would be undertaking an evaluation of the initiative once it ended. The education provider wants to use the learners' personal information collected during the initiative in the evaluation.

Can the education provider use the learner's personal information for evaluation purposes?

Yes. There is a direct relationship between delivering the initiative and evaluating its effectiveness. The learners who participated (and their parents) were informed that the education provider would be completing an evaluation of the initiative. Therefore, the learners (and their parents) would reasonably expect their personal information collected through the delivery of the initiative to be used for evaluation purposes.

Example – Using emergency contact information (not directly related)

A school holds emergency contact information so that they can contact appropriate people when an emergency occurs at the school. Learners may have multiple emergency contacts, and emergency contacts can include individuals other than the learner's parents or guardians (e.g. grandparents, caregivers).

Each year the school runs a couple of fundraising initiatives to support the purchase of school equipment. The school administrator wants to use the emergency contact information it holds to send out communications about the schools upcoming fundraising initiative. As the emergency contact information contains a broader range of people than parents and caregivers, the school administrator believes they can reach more potential donor's using this information.

Can the school use the emergency contact information for this secondary purpose?

No. While fundraising activities are an important source of funding for schools and ECE services, using emergency contact details to communicate about fundraising activities would not be a directly related purpose to the original purpose the emergency contact information was collected. The relationship between the two purposes is not immediate, and it is unlikely that the emergency contacts would expect their information to be used for this secondary purpose.

Serious threat exception

If you believe a child or young person is in immediate danger, call the Police on 111.

Where you want to use information that you hold about a learner for wellbeing and safety or family harm purposes check whether section 66C of the Oranga Tamariki Act 1989 or section 20 of the Family Violence Act 2018 apply. If those sections don't apply, then you can consider whether the IPP 10 serious threat exception applies.

To rely on the serious threat exception, you must be satisfied that a serious threat exists **and** believe on reasonable grounds that the information requested is necessary to prevent or lessen that threat.

The exception provides for two types of threats:

- to public health or safety

  or

- the life or health of a learner or another person.

When is a threat serious?

There are three factors that need to be considered when deciding whether a threat is serious:

- the likelihood of the threat occurring
- the severity of the consequences if the threat occurs
- the time at which the threat might occur.

All three factors don't need to be present to reach the threshold of serious threat. For example, if there is a high likelihood of the threat occurring and the severity of the consequences are significant (factors 1 and 2), but it is unclear when the threat may eventuate (factor 3), the serious threat threshold will likely be met. The test is what a reasonable person would consider to be serious in the circumstances, having considered all three factors.

A serious threat assessment will be situation specific and should consider all relevant circumstances, including those of the learner or learners concerned. A serious threat can arise for one learner based on the relevant risk factors of that learner but may not meet the threshold in relation to a different learner.

For example, a threat of harm to a learner may more readily meet the threshold of serious harm due to a learner's age and not being able to act independently and make their own decisions.

Is using the information necessary to lessen the threat?

Once you have decided that a serious threat exists, you need to determine whether your proposed use of the learner's personal information is necessary to prevent or lessen the threat. You should ask yourself whether not using the information

requested would increase the likelihood of the serious threat occurring – for example:

- is the information relevant or needed to address and lessen the serious threat
- how will using the information do this
- are you in a position to respond to and lessen the serious threat?

Example – Disease outbreak

An outbreak of measles has been declared by Health NZ in a region of NZ. There are several children and young people who have contracted measles within the regions, all of whom were attending school or an early learning centre.

Can the schools or ECE services use information they hold about their learners to control and manage the outbreak within their environment?

Measles is a highly contagious disease that can cause harm to health of children and young people. When an outbreak is declared by Health NZ it confirms that measles has been circulating in the community creating a serious threat to the health of individuals, particularly children and young people. Therefore, the threat is already occurring (factors 1 and 3), and the severity of the consequences are high (factor 2). In this case, a serious threat exists.

When there is a declared outbreak, schools and ECE services will need to take all reasonable measures they can to protect their learners. In this situation, the serious threat threshold has been met. There are reasonable grounds to believe that using the health and medical information (for ECE services, this may include vaccination records) they hold will assist them to identify vulnerable learners and prevent or lessen the threat of the outbreak for their learners. For example, schools and ECE services could identify learners who could be more vulnerable if they were to contract measles and develop plans to ensure those learners can continue to receive education services safely (e.g. remote learning).

When your use of a learner's information doesn't identify them

IPP10 provides two exceptions where personal information about a learner can be used if you believe on reasonable grounds that the information will be used:

- in a form in which the learner cannot be identified

  or
- for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the learner.

Checklist for de-identifying a learner's personal information

These two IPP10 exceptions require you to de-identify or anonymise learner data before you use it or publish your research or statistics.

De-identifying a learner's personal information enables you to use that information for secondary purposes while ensuring a learner's privacy is protected and respected. De-identifying requires more than just removing their name from the information.

You can use the following checklist to make sure you have de-identified your learner's personal information properly.

Remove direct identifiers like:

- learner names, including initials and nicknames
- National Student Number (NSN) and other unique identifiers
- year level
- address, contact details, email address, links to social media pages
- photos, videos, audio and voice recordings.

Remove indirect identifiers like:

- unique achievements (e.g. prizes won, scholarships awarded)

- specific family details (e.g. details of parents and siblings)
- community or cultural references specific to a learner or small group of learners
- combination of information (e.g. Year 13 head girl who captains the cricket team).

Generalise or aggregate:

- replace learner names with unique codes if you need to track results over time (e.g. learner A, B, C or Learner 001, 002, 003)
- use totals, ranges or percentages instead of individual scores (e.g. 10 learners scored 80 – 90% on the Year 11 internal maths assessment)
- group by categories instead of specifics.

Be mindful of using digital technologies to de-identify your learners' information. Only digital technologies approved for use by your education provider should be used. This ensures that the digital technologies you are using are privacy protective.

For more information on digital technologies see Chapter 16: Digital Technologies.

Once you have de-identified your information or dataset, sense check it before you use it. Ask yourself:

- Could another person reasonably be expected to identify the learner or learners?
- Does the context in which the information is placed make it obvious who the learner is or learners are?

Your de-identified information or dataset should be store securely and separate from the original identifiable information

Example – Research project for tertiary study

A teacher at a primary school is undertaking tertiary study which requires the completion of an education related research project. The teacher wants to look at the impacts of maths anxiety in Year 6 learners. The teacher would like to use the maths progression and achievement information of the learners at the school to inform part of her research.

Can the teacher use the Year 6 learners' information?

No. The teacher is completing the research project in their personal capacity not as part of their role as a teacher at the school.

The teacher would need to make a request to the school to share the learners' information. The school would then need to consider whether an IPP 11 exception applied that would enable the information requested to be shared with the teacher (e.g. the research and statistics exception).

While the school wouldn't require the learners' (or their parents where appropriate) authorisation (consent) to share their information, it would be good practice to let them know that their information is being shared with the teacher for research purposes.

Example – Exemplars used for training and professional development purposes

Learners at an intermediate school submit essays for assessment. The school principal wants to use some of the graded essays as examples of how to correctly complete an assessment of essays (as a secondary purpose). The graded essay exemplars will be used to help other teachers undertake marking of essays to the standard expected and ensure consistency of marking across the school.

Can the principal use the learner's marked essays?

The school principal can use a learners' marked essays for this secondary purpose so long as the essays are used in a form which does not identify the learner. All identifying information must be removed from the essay e.g. the learner's name, national student number.

If parts of the essay content can identify the individual, then any information that can be used to identify the learner should be removed. If removal of that information would make the essay unusable for the secondary purpose, then the essay should not be used.

Using information for wellbeing, safety, or family harm purposes

The following sections provide guidance on how to use information under the Oranga Tamariki Act 1989 and the Family Violence Act 2018.

If you believe a child or young person is in immediate danger, call the Police on 111.

Oranga Tamariki Act 1989

Section 66C of the Oranga Tamariki Act permits Child Welfare and Protection Agencies (CWPAs) or Independent Person to use information they hold about learners for specified purposes related to their wellbeing and safety.

Schools and ECE services are CWPAs under the Oranga Tamariki Act. Other agencies, organisations or individuals working within the education sector may also be a CWPA or Independent Person, but you should check to ensure you meet the

definition of CPWA or Independent Person under the Act before you use a learner's information for the purposes set out in section 66C.

Section 66C enables you to use information you hold about a learner for specified purposes, including:

- preventing harm or neglect to a child or young person
- Family Group Conferences and other care and protection work
- making, carrying out, or reviewing a risk assessment, needs assessment, prevention plan or support plan for a child or young person
- external services facilitated by Oranga Tamariki for a child or young person and their family or whānau.

You do not need consent of the learner (or their parent where appropriate) to use the information you hold about them for one of the purposes set out in section 66C.

You should always consider the best interests of the learner when using their information for section 66C purposes – in some cases it may be in their best interests to let them know, in other cases it could expose them to additional risk and harm.

For more detailed guidance on **sharing** information under the Oranga Tamariki Act 1989 see:

- Chapter 7: Sharing Information.
- Sharing information for the wellbeing and safety of children and young people guidance.

Family Violence Act 2018

Section 20 of the Family Violence Act 2018 permits the use of personal information between Family Violence Agencies (FVAs) and Social Sector Practitioners (SSPs).

School boards and ECE services are FVAs under the Family Violence Act. Other agencies, organisations or individuals working within the education sector may also be a FVA or SSP, but you should check to ensure you meet the definition of a FVA or SSP under the Act before you share information under section 20.

A Charter School does not meet the definition of a Family Violence Agency under the Family Violence Act 2018. For the purposes of section 20, a registered teacher working at a Charter School is a Social Sector Practitioner.

Section 20 enables you to use information you hold about a learner for specified purposes, including:

- to help ensure that a victim is protected from family violence
- to make or contribute to a family violence risk or needs assessment
- to make, or contribute to the making or carrying out of, a decision or plan relating or responding to family violence.

You do not need to obtain consent of, or consult with, the learner (or their parents where appropriate) to use their information for one of the purposes set out in section 20.

You should always consider the best interests of the learner when using their information for section 20 purposes – in some cases it may be in their best interests to let them know, in other cases it could expose them to additional risk and harm.

For more detailed guidance on **sharing** information under the Family Violence Act 2018 see:

- Chapter 7: Sharing Information.
- Sharing information for the wellbeing and safety of children and young people guidance.

Sharing information

Information sharing is a critically important activity within the education sector.

Education providers will often need to work together to ensure learners are getting the services and supports they need to succeed through their education journey. This means making sure that relevant information is available to the right people at the right time in the right way.

Information sharing can occur in various ways. For example:

- one-off share of information about a learner
- a one-off share about multiple learners
- ongoing sharing of information about one or multiple learners
- between different education providers e.g. between schools, schools and ECEs, or schools, ECEs and service providers
- within an education provider e.g. between teachers, between a principle and a teacher or between a school and a learner (or their parents).

When sharing information about learners, you need to get your privacy thinking right. Not doing so can cause real harm (in the short term and long term) and undermine trust and confidence in the sector. Failing to think things through properly can also impact learner engagement and achievement.

Good information sharing practices:

- create transparency and build trust and confidence in how education providers are sharing personal information

- enable the delivery of effective, learner specific services and supports that improve educational outcomes
- build awareness within an education provider of what information is being shared, who the information is being shared with, and for what purpose
- support people working in the education sector to make good judgment-based decisions when sharing a learner's information.

Different ways to share information about learners

All information sharing must be permitted by legislation. A legislative provision that permits the sharing of information is referred to as the 'legal authority'.

There are various legal authorities that permit the sharing of information about learners for a variety of purposes, for example:

- The Privacy Act 2020 permits personal information about learners to be shared for a number of specified purposes.
- The Oranga Tamariki Act 1989 enables sharing of information about learners for specified wellbeing and safety purposes.
- The Family Violence Act 2018 enables sharing of information about learners for specified family violence purposes.
- The Education and Training Act 2020 also permits information sharing for specified purposes.

Knowing what you can share, when, and with whom can feel challenging, especially if there is urgency e.g. there are wellbeing or safety concerns about a learner, or the needs of the learner are complex.

This chapter provides the information you need to make good decisions when sharing information about your learners.

How this chapter is set out

This chapter is broken down into the following sections:

Legal Frameworks for Sharing

- Sharing under the Privacy Act 2020
- Sharing under Oranga Tamariki Act 1989
- Sharing under the Family Violence Act 2018
- When you are required to share information

An information sharing frameworks quick reference guide can be found here: Office of the Privacy Commissioner | Quick reference guide: Information sharing frameworks.

Information Sharing in Practice

- Sharing with other education providers
- Sharing within an education provider
- Education providers sharing with service providers
- Sharing with parents
- Sharing in emergencies
- Sharing with education agencies
- Sharing at multi-agency meetings

Sharing under the Privacy Act 2020

Information privacy principle (IPP) 11 permits the sharing of personal information that is held by education providers in certain circumstances.

For more information about the Privacy Act 2020 and the information privacy principles (IPPs) see Chapter 2: The Privacy Act and personal information.

For guidance on sharing information using the other Privacy Act mechanisms see: What legal authority to use | NZ Digital government.

Relevant information privacy principles

The Privacy Act refers to “disclosing” information. The relevant information privacy principles (IPP) for sharing or disclosing personal information are:

Principle 11: Limits on disclosure of personal information

An education provider that holds personal information must not disclose the information to another agency or to any person unless it believes on reasonable grounds that an exception applies.

Principle 8: Accuracy of personal information to be checked before use or disclosure

An education provider that holds personal information must not use or disclose that information without taking steps that are reasonable, in the circumstances, to ensure that the information is accurate, up to date, complete, relevant and not misleading.

When you want to share information that you hold for learner wellbeing or safety purposes you should consider section 66C of the Oranga Tamariki Act before deciding whether an IPP10 exception applies.

See: Sharing under Oranga Tamariki Act 1989.

When you want to share information that you hold about a victim or perpetrator of family violence you should consider section 20 of the Family Violence Act before deciding whether an IPP10 exception applies.

See: Sharing under Family Violence Act 2018.

When using an IPP11 exception to share personal information you are not limited to sharing with Child Welfare and Protection Agencies, Independent Persons, Family Violence Agencies or Social Services Practitioners. This can

be useful for multi-agency meetings where a wider group of agencies and organisations need to be present.

Information Privacy Principle (IPP) 11 enables you to share personal information (either proactively or on request) with another agency or person in certain circumstances (exceptions).

IPP11 requires that an agency believes on reasonable grounds that one of the listed exceptions applies.

IPP11 exceptions

IPP11 contains a number of exceptions. The exceptions that commonly apply within the education sector include:

- The purpose for sharing is one of the purposes, or directly related to one of the purposes, for which the information was obtained.
- The learner (or their parent where appropriate) has authorised the sharing of their information.
- The information being shared is being used in a way that does not identify the learner.
- The information is required by law (e.g. section 66 of the Oranga Tamariki Act).
- Sharing the information is necessary to prevent or lessen a serious threat to the learner's life or health, or public health and safety more broadly.
- Sharing the information about the learner is necessary to uphold or enforce the law.

What you need to consider when applying an IPP11 exception

Deciding whether an IPP11 exception applies will be a judgement call and will depend on the circumstances. To help you decide whether an IPP11 exception applies in the circumstances you should consider:

- Are there reasonable grounds to believe that the exception applies in the circumstances?
- Is sharing of the information necessary to achieve the purpose of the exception?
- Could harm result from sharing, or not sharing, the information?
- Is the recipient the appropriate agency or person to share the information with?
- Is the information being shared particularly sensitive in nature?
- Is the information you are intending to share current and up to date?
- Is sharing the information is in the best interests of the learner at this time?

The following sections look at some of these considerations in more detail.

You must believe on reasonable grounds that an exception applies

To rely on an IPP11 exception, you **must**:

- believe that the exception applies at the time you are sharing the information **and**
- your belief must be reasonably held.

The means you need to consider whether the exception applies before you share the information, and you must have properly considered all the relevant information in the circumstances.

Whether there is a reasonable basis will depend on:

- what you know about the circumstances of the learner
- what you have been told by the requestor about why the information is required
- what information is being requested about the learner.

When you are sharing a learner's information in response to a request, the requestor advising you that an exception applies is not sufficient for believing on reasonable grounds that an exception applies – you need to come to reasonable belief yourself.

If you do not have enough information to decide whether the IPP11 exception applies you should ask the requestor for additional information. If there is some urgency to the request, it might be quicker to call the requestor and seek the additional information over the phone.

Some exceptions require you to consider necessity

The IPP11 exceptions for exceptions for preventing or lessening a serious threat and maintenance of the law and also require you to consider whether sharing the information is necessary in those specific circumstances.

Whether the sharing of the information for these specific exceptions is necessary is a relatively low threshold - is the use of the information needed or required in the circumstances, or required for a given situation?

To help determine whether the sharing of information is necessary you should consider whether not sharing the information could, in the circumstances:

- increase the likelihood of the serious threat occurring (e.g. an infectious disease spreading throughout the community)

  or
- compromise a law enforcement agency's ability to maintain the law (e.g. investigate suspected offending).

Is the information accurate, up to date, relevant, complete and not misleading?

IPP8 requires that you take reasonable steps to ensure information is accurate, up to date, complete, relevant, and not misleading before you share it with another agency or person.

Sharing inaccurate, out of date or misleading information can result in prejudicial information about the learner being used by people to make decisions about them. This can have significant short- and long-term impacts for the learner and potentially their family or whānau.

Take the time to check the information is accurate, up to date, relevant, complete and not misleading before you share it.

Make sure you are sharing the latest versions of documents or learner records.

For more information about accuracy see Chapter 10: Accuracy of information.

Can I share sensitive personal information?

The Privacy Act does not define or provide rules around sharing sensitive information. However, in practice special care should be taken when sharing intimate or particularly sensitive personal information about a learner. Sensitive information is information that has some real significance to the learner, is revealing, or generally relates to matters they might wish to keep private.

However, there may be situations where the sharing of sensitive information is necessary – for example, when there is a serious threat to a learner's life or health. The relative sensitivity of the information, and whether it is in the best interests of the learner, will be an important consideration when thinking about sharing sensitive information under an IPP11 exception.

Read more information about sensitive personal information and the Privacy Act.

In some cases, the information being requested may include information of such a sensitive nature that it would be appropriate for that information to be requested using a production order or a search warrant. A production order or search warrant provides assurance that the sensitive information is relevant and necessary for the purposes for which it is being requested and shared.

Do I need consent to share under an IPP11 exception?

One of the IPP11 exceptions is the authorisation (consent) of the individual. This means that you can obtain the authorisationof the learner (or their parents where appropriate) to share their personal information for a secondary purpose.

When relying on another IPP11 exception, you **do not** need the consent of the learner (or their parent where appropriate) to share their information.

For more information about obtaining consent to share a learner's personal information see: Authorisation (consent) in practice.

Can I decline a request to share information?

If, after considering the circumstances of the request, you are not satisfied that there are reasonable grounds to share the information under one of the IPP11 exceptions, you should decline the request.

However, there may be another legal authority that permits you to share the information, (e.g. section 66C of the Oranga Tamariki Act 1989 or section 20 of the Family Violence Act 2018). You should always consider whether these provisions apply in the circumstances, especially when the purpose of sharing the information is to keep a learner safe.

Just because you have a legal authority to share a learner's information doesn't always mean you should. You can also decline the request to share information for other reasons, such as:

- Sharing at this time may not be in the best interests of the learner.
- You may have assured the learner (or their parents where appropriate) that you will keep their information confidential.
- You may be subject to other legal, ethical or professional standards that require you to maintain confidentiality.

For more information on confidentiality see Chapter 4: Privacy and confidentiality.

You can't decline a request to share information when you are required to provide the information by law.

See: When you are required to share information.

Keep good records

It is important to keep good records of your information sharing activities. At a minimum you should record:

- the request you received and from whom (including receipt and response date)
- any additional information you requested from the requestor
- your decision whether, or not, to share the information requested
- the IPP11 exception you relied on to share the information, including the information you considered to form the reasonable belief that the exception applied in the circumstances
- the information that you shared.

An easy way to do this is to create an Information Sharing Register. This can be as simple as an excel spreadsheet. Registers will contain personal information, and in some cases sensitive information. It is important to keep your information sharing record secure (e.g. password protect your spreadsheet) and limit access to only those that need to have access.

Using IPP11 exceptions in practice

This section provides some examples of sharing learner information under the IPP11 exceptions in practice.

Authorisation (consent) exception

IPP11 provides an exception where personal information you hold about a learner can be shared if the learner (or their parents where appropriate) provides authorisation (consent).

You will need to consider whether the learner is old enough to be able to authorise (consent to) the intended sharing of their information. Where the learner is younger, or not sufficiently able to understand, then you should obtain authorisation (consent) from the learner's parents.

For a learner (or their parents where appropriate) to provide authorisation to share their personal information you will need to ensure that they have sufficient information to make an informed decision.

Obtaining authorisation (consent) can be done through:

- a **consent form** (where a learner or their parent can explicitly authorise (consent to) the intended sharing)
  or
- an **opt out form** (where information about a learner will be shared for a specified purpose unless the learner (or their parents where appropriate) opts out).

You should attach the collection privacy statement to the consent or opt out form. The privacy statement will provide the learner (or their parents where appropriate) with the information they need to make an informed decision to authorise the sharing of their information. You should also provide a link to your privacy policy in your consent or opt out form so that learners (or their parents where appropriate) can have confidence in how you collect, use, share and protect personal information more generally.

Detailed guidance on how to inform learners and their parents can be found in Chapter 8: Keeping Learners and parents informed.

Authorisation is not a ‘one and done’ thing. Where authorisation has been provided, learners (or their parents where appropriate) should be able to withdraw that authorisation at any time. Also, if it has been some time since the learner (or their parents where appropriate) provided authorisation for their information to be shared you should check whether they are still comfortable with the information being shared for that purpose.

Where you have concerns about a child or young person’s wellbeing or safety the Oranga Tamariki Act or the Family Violence Act you do not require the consent of the child or young person to sharing their information to keep them child safe from harm.

Read more about sharing under the Oranga Tamariki Act and the Family Violence Act.

When a learner (or their parents where appropriate) withdraws authorisation (consent)

A learner or their parents can withdraw authorisation they have **previously provided** for their information to be shared for specified purposes. For example, learners (or their parents where appropriate) may withdraw authorisation for their images to be posted on social media.

When a previously provided authorisation is withdrawn, you must stop sharing their information for the purpose to which the authorisation applied.

When you are relying on one of the other IPP11 exceptions, section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act, to share a learner’s personal information for a secondary purpose, the learner (or their parents where appropriate) will not be able to withdraw their authorisation. This is because their authorisation was not the basis relied on for sharing their information.

Example – withdrawing consent to share photos and videos

A school provides parents with a consent form where parents can consent to photos and videos of their child being taken and then consent to specific purposes for which those photos can be used or shared by the school. Purposes include posting learning-based activities to the school's social media platforms and parent communication platforms.

The school principal maintains a register of all photo and video consents and the purposes for which those photos and videos can be used. While parents can withdraw consent at any time, the principal requires parents to update their photo and video consents every year, and the school principal updates the register with any changes.

One year a learner's parents withdraw consent for staff at the school to take, use or share photos or videos of their child. They request that any photos or videos held by the school are permanently deleted and all photos or videos of their child posted on parent communication platforms, or social medial platforms are removed.

What actions should the school principal take?

The school principal should:

- Update the school photo and video consent register recording that consent to collect, use or share the photos or videos of the learner has been withdrawn.
- Review the parent communication and social media platforms and identify all posts where the learner is identified in photos or videos and remove those images.
- Remove the photos and videos from the parent communication and social media platforms.
- Inform the parents of the learner of the actions that have been taken.
- Inform all school staff that any photos or videos taken should not include the learner.

- Review all photos and videos before they are posted to the parent communication or social media platforms to ensure photos or videos of learners where no consent to collect, use or share the images exist are not inadvertently posted.

For more information on retention and disposal of information see Chapter 12: Retaining and deleting information.

For more guidance on taking photos and videos of children see our guidance: Office of the Privacy Commissioner | Children and young people: photography and filming guidance.

Law enforcement exception

To rely on the law enforcement exception, you must believe in reasonable grounds that sharing information is necessary to avoid prejudice to the maintenance of the law including prevention, detection, investigation, prosecution and punishment of offences.

This exception supports the maintenance of criminal and regulatory enforcement processes. It does not give Police or other law enforcement agencies the right to access any information. The exception applies to situations where **not** providing specific and relevant information would prejudice or be detrimental to enforcing the law.

In the early stages of an investigation into an offence, a law enforcement agency may not have sufficient information to apply for a production order or a search warrant. This can make it difficult to progress a criminal or regulatory investigation. A request for information using the law enforcement exception may be the only practical means of obtaining the information necessary to effectively investigate the offending, particularly during the initial stages of an investigation.

The law enforcement agency requesting information must show a link between the offence(s) being investigated and the relevance of the information being requested - simply asserting that the information is needed for a law enforcement agency investigation is not sufficient. You need sufficient details to form a reasonable belief that sharing the information is necessary for the purpose for which it is being requested. Without this information, you will not be able determine that the law enforcement exception applies.

To help decide whether sharing the information is necessary, you should ask yourself what the effect would be if the information requested by the law enforcement agency was not provided – for example, would not sharing the information compromise the ability of the law enforcement agency to do their job?

For more detailed guidance on the law enforcement exception see our guidance: Releasing personal information to Police and law enforcement agencies.

Example – not enough information/decision to share

A school administrator receives an email from a constable from the local police station requesting the home address and parent contact details of a learner. The email has come from the constable's police email address. The constable advises that the information is being requested under IPP11(1)(e) of the Privacy Act (the law enforcement exception).

Can the school share the information requested with the constable?

While the constable has advised the request is being made under the IPP11(1)(e)(i) of the Privacy Act, it is for the school to determine whether the information requested is necessary for the purpose under IPP11(1)(e)(i) – upholding or enforcing the law.

In this case, the constable has not provided sufficient information about the offence being investigated and the relevance of the information being requested to

investigating that offence. Without this information, the school administrator cannot be satisfied that the information is necessary for upholding or enforcing the law.

The school administrator should ask the constable for more information to help them determine whether the law enforcement exception applies in the circumstances. For example, the school should ask what offending is being investigated, and why the home address and contact details of the learner's parents are relevant and necessary for purposes of investigating that offence. Once the school has received this information it will then be able to determine whether not sharing the information requested would prevent the investigation into the offence(s) commencing or continuing.

Police do have an information request form that includes all relevant information to support the request – if they haven't provided the form, ask them to do so.

If the constable advises that Police are investigating on-going thefts of vehicles in the area by a group of youth, and up to date address and contact information for the learner and their parents is necessary to enable Police to contact the learner and their parents as part of the investigation, it would be reasonable for the school to rely on the law enforcement exception to share that information with the constable. Not providing the information would impact Police being able to continue its investigation into the offending.

Serious Threat Exception

If you believe a child or young person is in immediate danger, call the Police on 111.

To rely on the serious threat exception, you must be satisfied that a serious threat exists **and** believe on reasonable grounds that the information requested is necessary to prevent or lessen that threat.

The exception provides for two types of threats:

- to public health or safety

  or

- the life or health of a learner or another person

When is a threat serious?

There are three factors that need to be considered when deciding whether a threat is serious:

- the likelihood of the threat occurring
- the severity of the consequences if the threat occurs
- the time at which the threat might occur.

All three factors don't need to be present to reach the threshold of serious threat. For example, if there is a high likelihood of the threat occurring and the severity of the consequences are significant (factors 1 and 2), but it is unclear when the threat may eventuate (factor 3), the serious threat threshold will likely be met. The test is what a reasonable person would consider to be serious in the circumstances.

A serious threat assessment will be situation specific and should consider all relevant circumstances, including those of the learner or learners concerned. A serious threat can arise for one learner based on the relevant risk factors to them but may not meet the threshold in relation to a different learner.

For example, a threat of harm to a learner may more readily meet the threshold of serious harm due to a learner's age or ability to act independently and make their own decisions.

Is sharing the information necessary to lessen the threat?

Once you have decided that a serious threat exists, you need to determine whether sharing the learner's personal information is necessary to prevent or lessen that

threat. You should ask yourself whether not sharing the information requested would increase the likelihood of the serious threat occurring – for example:

- Is the information requested relevant or needed to address and lessen the serious threat?
- How will sharing the information do this?
- Is the person receiving the information in a position to use the information to respond to and lessen the serious threat?

Example – Disease outbreak (decision to share)

An outbreak of measles has been declared by Health NZ in a region of NZ. There are several children and young people who have contracted measles within the regions, all of whom were attending school or an early learning centre.

The National Public Health Service (NPHS) is contacting all schools and ECE services within the region requesting the names, dates of birth and immunisation information of all learners currently enrolled. The NPHS has advised the schools and ECE services that the enrolment information will be used for the purposes of identifying the number of vaccinated and unvaccinated children and young people. This information will assist the NPHS determine the level of risk in the community and ensure prevention and containment resources are allocated effectively and in a timely manner.

Can the schools or ECE services share the information with the NPHS?

Measles is a highly contagious disease that can cause harm to the health of children and young people. When an outbreak is declared by Health NZ it confirms that measles has been circulating in the community creating a serious threat to the health of individuals, particularly children and young people. Therefore, the threat is already occurring (factors 1 and 3), and the severity of the consequences are high (factor 2). In this case, a serious threat exists.

When there is a declared outbreak, local health authorities need to take actions to prevent or lessen the spread of the disease. To do that, they need information about learners in the affected area, including immunisation information. Obtaining names and dates of birth of learners attending the schools and ECE services in the affected area will enable NPHS to match the information against the immunisation register. This information will help them determine the level of risk across the community and ensure appropriate containment and prevention measures are implemented.

In this situation, the serious threat threshold has been met. There are reasonable grounds to believe that sharing the names and dates of birth of learner's the affected area is necessary to help prevent or lessen the serious threat, and the NPHS (the requestor) is able to use the information to prevent or lessen that threat.

Example – Missing learner (decision to share)

The Police are trying to locate a year 10 learner who has been reported missing by their family after failing to return home from school. The learner has a history of mental health challenges and has been missing over 48 hours. The learner does not have their phone with them, so Police has been unable to obtain location data from the telecommunications provider.

The learner's school has an online learning platform which enables learners to message each other and their teachers. The learner also has a school email address which they use as their main email account. Police make a request to the school principal for the learner's messaging and email history over the last month. The Police advise the principal that the email and messaging history will help them to determine where the learner might be. The Police have made the request to the school relying on IPP11(1)(f)(ii) – serious threat to an individual.

Can the school principal release this information to the Police?

While the Police has advised the request is being made under the IPP11(1)(f)(ii) of the Privacy Act, it is for the school principal to determine whether the information requested is necessary for that purpose – preventing or lessening a serious threat to the life or health of an individual.

To rely on the serious threat exception, the school principal needs to have a reasonable belief that there is a serious threat to the learner's life or health and that the sharing of the information is necessary to prevent or lessen that threat. To do that the principal first needs to determine whether there is a serious threat by considering the likelihood of the threat occurring, the severity of the consequences if the threat occurs, and the time at which the threat might occur.

Given the learner's age, the mental health concerns and the length of time they have been missing, there are reasonable grounds to believe that there is a serious threat to their life or health if they cannot be located.

Next, the school needs to determine whether sharing the learner's email and messaging information is necessary to prevent or lessen that threat. The emails and messages may provide information about why the learner has not returned home, and where they may be. This information could help Police locate them. The request is also limited to emails and messages in the previous month – recent emails and messages are likely to be more relevant to locating the learner. Not sharing the information could delay the Police locating the learner which could lead to serious harm to the learner's health or safety.

In this case, it would be reasonable for the school principal to rely on the serious threat exception to share the learner's emails and messaging from the past month with Police.

Sharing under the Oranga Tamariki Act 1989 (wellbeing and safety purposes)

If you believe a child or young person is in immediate danger, call the Police on 111.

The following sections provide guidance on how to share information under the Oranga Tamariki Act.

Raising or reporting concerns

If you believe that a learner has been or is likely to be harmed, ill-treated, abused, neglected, or deprived or you have concerns about the wellbeing of a learner, section 15 permits you to share information about your concerns directly with Oranga Tamariki.

When you make a Report of Concern in good faith you are protected from civil, criminal or disciplinary proceedings.

You can discuss and share your concerns with Oranga Tamariki by calling 0508 326 459 or by emailing contact@ot.govt.nz.

When you are required to share (section 66)

Oranga Tamariki or Police can require an agency or individual to provide relevant information if that information is required:

- to determine whether the child or young person needs care or protection or assistance

  or
- for any proceedings under Part 2 of the Oranga Tamariki Act (including a Family Group Conference).

When you receive a section 66 request you **must** provide the information specified in the request (unless the information is covered by legal professional privilege). Unlike section 66C, you do not need to consult the learner (or their parents) before you provide the information under a section 66 request.

If you are unsure whether the request is being made under section 66, or what the purpose of the request is, you should ask the requestor for this information before you share the information with them.

When you want or are asked to share (section 66C)

Section 66C of the Oranga Tamariki Act permits the sharing of information about a child or young person for specified wellbeing and safety purposes.

Under section 66C you can proactively share information, or you can share information in response to a request from a CWPA or Independent Person.

Sharing information under section 66C is broader than sharing safety concerns about a child or young person through a report of concern with Oranga Tamariki or Police. Section 66C provides for the sharing of information to support the wellbeing of children, young people and their family as early as possible.

Who you can share with

Section 66C of the Oranga Tamariki Act permits Child Welfare and Protection Agencies (CWPAs) or Independent Persons to share information about a child or young person with other CWPAs or Independent Persons for specified wellbeing and safety purposes.

Child Welfare and Protection Agencies (CWPAs) are a group of organisations, and therefore their employees, or volunteers including:

- Any social, family and community service that provides services under section 396 of the Oranga Tamariki Act.

- Any person, body or organisation that provides regulated services under schedule 1 of the Children's Act 2014.
- Housing New Zealand Corporation.
- Ministry of Education, schools and early childhood education services.
- Ministry of Health, Health NZ and health providers.
- Ministry of Justice.
- Department of Corrections.
- Ministry of Social Development.
- Oranga Tamariki – Ministry for Children.
- New Zealand Police.

Independent Persons are professionals or people including:

- A practitioner under the Health Practitioners Competence Assurance Act 2003 who provides health or disability support services.
- A Children's Worker (under section 23(1) of the Children's Act).
- A person or class of persons designated as an independent person by regulations made under section 447(1)(ga)(ii) of the Oranga Tamariki Act.

Schools and ECE services are CWPAs under the Oranga Tamariki Act.

Other agencies, organisations or individuals working within the education sector may also be a CWPA or Independent Person, but you should check to ensure you meet the definition of CPWA or Independent Person under the Act before you share information for the purposes set out in section 66C.

If you want to share information with an agency or person that is not a CWPA or Independent Person, you may be able to share information with them under the Privacy Act.

For more information on who section 66C applies to see: Information-sharing-Guidance-OT-Act-1989.pdf (appendix one).

The purposes for which you can share

Section 66C enables information about a learner to be shared for specified purposes, including:

- preventing harm or neglect to a child or young person
- for Family Group Conferences and other Care and Protection work
- making, carrying out, or reviewing a risk assessment, needs assessment, prevention plan or support plan for a child or young person
- external services facilitated by Oranga Tamariki for a child or young person and their family or whānau.

Section 66C enables sharing between any CWPA and/or Independent Persons e.g. between a school and the Ministry of Education, between an ECE and a school, between a school and a health care provider.

If you are unsure of the purpose for which the information is being requested, you should ask the requestor for this information before you decide to share any information with them. If you do not know the purpose you will not be able to determine whether one of the purposes in section 66C applies, and what information is necessary to share with the requestor.

What does wellbeing and safety mean in practice?

Wellbeing of a child or young person includes:

- strong positive whānau relationships
- spiritual and cultural connections
- having their developmental needs met and supported – education, behaviour, life skills and self-care skills
- emotional resilience and support
- social and peer groups that are supportive, caring and positive,
- physical and mental wellness

- security – being safe from harm, living in a safe community, having a warm dry home, having enough food.

Safety concerns include:

- physical, emotional, sexual abuse, deprivation, neglect, and ill-treatment
- situations where parents or caregivers aren't willing or able to care for the child, where a child is subject to family harm (including where they are exposed to it)
- and where the development of a child or their physical, mental or emotional wellbeing is likely to be impaired or neglected in a way that is avoidable.

Not all wellbeing issues will be safety issues, but if there is a safety concern, a child or young person's wellbeing will be affected.

Where you have concerns about a child or young person's safety you should make a report of concern to Oranga Tamariki or the Police.

What information is relevant?

You can share information that you believe is relevant to help achieve one or more of the purposes set out in section 66C. Deciding what information is relevant will often be a judgement call and depend on the circumstances of each situation.

Things to consider when deciding whether information is relevant include:

- your knowledge of the learner and their circumstances including information about:
  - the learner themselves
  - their home environment
  - their needs, aspirations, strengths

  - challenges they are experiencing (financial pressures, housing, family harm, health, access to education and learning difficulties)
  - support they have or are receiving – what worked well, what didn't work well and why
  - information about other people they have a relationship with such as their parents, wider family and whānau, teachers, doctors, sports coaches

- the person making the request, the purpose for which they are requesting the information and what they will be able to do with the information to support the learner
- the age of the information – older information may be out of date and therefore less relevant to the current circumstances or needs of the learner
- the context of the information – could the information be misinterpreted by the recipient without additional context?

There aren't any limits on who the information can be about. You can share information about a learner, their family or other people they have a relationship with if you believe it is relevant to protecting their wellbeing or keeping them safe.

If you are unsure whether information you hold may be relevant, talk to the requestor or the person you want to share the information with. Together you may be able to identify what information is relevant in the circumstances.

Consent to share is not required

You **do not** need to obtain the consent of the learner (or their parents or legal guardian where appropriate) to share their information under section 66C.

Requirement to consult with the learner

Section 66K of the Oranga Tamariki Act requires you **to consult** with the learner either before, or as soon as possible after, you share their information where it is practicable or appropriate to do so. Where a learner is very young or may not be

able to understand why you want to share their information, you should consult with their parents or legal guardian if it is appropriate and safe to do so.

This ensures that the learner is aware that their information is being shared, with whom, and what that person is going to do with their information. It also gives them the ability to share any concerns they may have about their information being shared.

You are required to consider their views before you share their information. While you can still share information if they strongly disagree, if their concerns relate to their wellbeing or safety, you should consider whether sharing the information with the requestor is in the learner's best interests at that time. You may need to advise the requestor of the wellbeing or safety concerns the learner has raised to ensure the sharing of the information doesn't place them at risk of further harm.

Examples of when it may not be practicable or appropriate to consult with a learner include:

- they are not developmentally able to understand (remember even young children can understand sharing information if you talk to them in an age-appropriate way)
- it might put them or someone else at risk of harm
- it might distress or upset them, or have a negative impact on their wellbeing
- it could get in the way of a Police investigation or prosecution
- you need to share information quickly because tamariki might be harmed otherwise
- after making reasonable efforts you, or another professional, can't get in touch with them, and you still think sharing is important to protect tamariki from harm.

You should always record the reasons why you decided not to consult with the learner.

Sharing information about multiple learners

When sharing information about multiple learners (e.g. sharing datasets or sharing information at multi-agency meetings), you are still required to consult with each individual learner prior to sharing their information where it is practicable or appropriate to do so.

Just like when sharing information about a single learner, whether it is impracticable or inappropriate to consult should be considered when you are developing the dataset or setting up your multi-agency meeting. For multi-agency meetings, each meeting participant will need to determine whether it is impracticable or inappropriate to consult with the learner.

You should always record the reasons why you decided not to consult with the learner when sharing datasets or sharing their information at multi-agency meetings.

Sharing information in good faith

Sharing information under section 66C requires you to make a judgement call. Every circumstance will be different – in some cases you might decide to share, in others you might not. When you are under pressure, and a child or young person may be at risk, making these judgement calls can feel overwhelming.

The Oranga Tamariki Act provides protection from civil, criminal and disciplinary proceedings when you share information under section 66C unless you have shared in bad faith. Bad faith includes sharing information when you know you shouldn't.

Acting in good faith means you have:

- made your best effort to share in line with the relevant statutory provisions
- checked that the information you intend to share is relevant, accurate, up to date complete and not misleading
- undertaken measures to ensure the information is shared safely with the right person in the right role
- consulted with the learner (or their parents where appropriate) if it is safe and appropriate to do so.

Read the Oranga Tamariki factsheet about sharing information in good faith from their Information sharing resources page.

You are protected from civil, criminal and disciplinary proceedings if you have shared information under section 66C unless you have shared in bad faith.

Confidentiality obligations

Obligations of confidence protect information deemed to be confidential from unauthorised access and disclosure. However, obligations of confidence are subject to exceptions which include situations where a learner's wellbeing or safety is at risk.

You can consider sharing confidential information when sharing information under section 66C. However, you will need to ensure that:

- you are sharing for a purpose set out in section 66C
- the confidential information is relevant to that purpose
- you have consulted with the learner before you share their information.

Your professional code of ethics, industry code of conduct or employment agreement will set out what information is considered confidential, under what circumstances that information may be shared and what you need to advise the child or young person when you are collecting their information.

When advising a child or young person (or their parents where appropriate) that specific information, or categories of information, will be kept confidential you should always clearly inform them of the exceptions to that confidentiality i.e. the circumstances in which you may share that information.

For more information about privacy and confidentiality see: Chapter 4 Privacy and Confidentiality.

When the requirements of section 66C aren't met

If you determine that the requirements of section 66C have not been met, you can consider whether one of the following applies in the circumstances:

- Section 20 of the Family Violence Act 2018.
- a Privacy Act IPP11 exception.

Additional resources

For more guidance on sharing information to protect children and young people, including a section 66C checklist see: Office of the Privacy Commissioner | Sharing information to protect the wellbeing and safety of children and young people.

For more guidance on sharing information under the Oranga Tamariki Act, including a section 66C request template form see: Guidance for sharing information.

Keep good records

It is important to keep good records of your information sharing activities. At a minimum you should record:

- the request you received and from whom (including receipt and response date)
- any additional information you requested from the requestor
- your decision whether, or not, to share the information requested
- the specified purpose you shared the information
- whether you consulted with the learner, any views they shared with you, or the reasons why you didn't consult them
- the information that you shared.

An easy way to do this is to create an Information Sharing Register. This can be as simple as an excel spreadsheet. Registers will contain personal information, and in

some cases sensitive information. It is important to keep your information sharing record secure (e.g. password protect your spreadsheet) and limit access to only those that need to have access.

How does the Privacy Act apply to sharing under the Oranga Tamariki Act?

Section 66 and 66C authorise the sharing of personal information for specific purposes related to the wellbeing and safety of children and young people. This means that you don't need to rely on one of the exceptions to Information Privacy Principle (IPP) 11 to share the information with another CWPA or Independent Person.

However, section 66Q requires you to comply withIPPs 1, 4, 5, 6, 7, 8, 9 and 13 in the Privacy Act.

In practice, this means when you are **sharing** information under section 66C of the Oranga Tamariki Act, you must also ensure you:

- share information in a safe and secure way and protect it from unauthorised access, use and disclosure (IPP5)
- have taken reasonable steps to ensure the information is accurate, up to date, relevant, complete and not misleading information (IPP8)
- are mindful about sharing unique identifiers.

When you are **receiving** information requested or provided under section 66C of the Oranga Tamariki Act, you must also ensure you:

- are requesting the information necessary for a lawful purpose of your agency (IPP1)
- receive the information:
    - in a manner that is fair and not unreasonably intrusive on the child or young person's personal affairs (IPP4)

- in a safe and secure way and protect it from unauthorised access, use and disclosure (IPP5)
- only retain the information for as long as it is necessary to do so (Public Records Act and IPP9).

Learners (or their representatives) have the right to request access to and correction of their personal information under IPP6 and 7. If you correct personal information or attach a statement of correction to personal information that is also information that you have shared under the Oranga Tamariki Act, you must, so far as is reasonably practicable, inform that CWPA or Independent Person of the correction.

Using the Oranga Tamariki Act in practice

The following examples work through the application of section 66C of the Oranga Tamariki Act.

Example – ECE service and Oranga Tamariki social worker (decision to share)

An ECE service manager receives an email request from a social worker working for a Non-Government Organisation (NGO) that provides support services to families in need. The social worker states that the request is being made under section 66C of the Oranga Tamariki Act.

The social worker is requesting information about a 3-year-old who is enrolled at the ECE. The information requested includes parent contact details, attendance records, and any behaviour related incident reports over the last 12 months. The social worker advises that the information is required to complete a needs assessment and identify appropriate supports for the child.

Can the ECE service manager share the information with the social worker?

To use section 66C both parties must be a Child Welfare and Protection Agency or an Independent Person. The ECE service is a CWPA but should confirm with the social worker that either the NGO they work for is a CWPA or they themselves are an Independent Person.

Information can be shared if the information will be used for one of the purposes set out in section 66C. In this case, the social worker has stated the information will be used to complete a needs assessment for the child, which is a purpose under section 66C.

The ECE service manager should ensure that the information they share with the social worker is relevant to the purpose of completing a needs assessment and is accurate and up to date. The social worker has requested information covering the last 12 months. If there is older information that the manager believes is relevant to the needs assessment it can share that information also. If the manager is unsure whether the older information is relevant, they could contact the social worker and talk to them.

The ECE service manager doesn't need the consent of the learner's parents to share the information, but they must consult with the learner (unless it is not practical or appropriate to do so). At 3 years old, the learner is too young to understand the request and share their views. As such, the ECE service manager should consider consulting with the learner's parents if it is practical and appropriate to do so.

While section 66C provides the legal authority to share the information, the ECE service manager must still comply IPP1 and 4 (lawful purpose for collection, necessity, method of collection), IPP5 (security and storage), IPP6 and 7 (access and correction rights), IPP8 (accuracy), IPP9 (retention of information) and IPP13 (unique identifiers) requirements.

The ECE service manager should record the request, the date of the request, the information they shared with the social worker, and the views of the learner's parents if it was practical and appropriate to consult with them.

Example – School and Oranga Tamariki social worker (unclear request/decision to share)

A school principal has received an email request from an Oranga Tamariki (OT) social worker. The principal is aware that the learner is under the care of Oranga Tamariki and is currently in foster care. The request is for information about the learner's educational progress and achievement.

Can the school principal share the information with the OT social worker?

It is unclear from the email request whether the OT social worker is requesting the information under section 66 (mandatory) or section 66C (voluntary) of the Oranga Tamariki Act. Where it is unclear, the school principal should seek confirmation from the social worker. To assist, the principal could provide the social worker with the template request form and ask them to complete it (Forms to request information | Oranga Tamariki — Ministry for Children).

The school principal does not need the consent of the learner or their parents to share the information under section 66C. After confirming the request is a section 66C request and identifying the relevant information the principal must consult with the learner (or their parents) if it is practical and appropriate to do so. The principal should talk to the learner about the request, who made it, what information is being requested and what it will be used for. They should also let the learner know that they will be sharing the information and provide space for them to voice any concerns that they may have.

While section 66C provides the legal authority to share the information, the school must still comply with IPP1 and 4 (lawful purpose for collection, necessity, method of collection), IPP5 (security and storage), IPP6 and 7 (access and correction rights), IPP8 (accuracy), and IPP13 (unique identifiers) requirements. The school must also comply with the retention requirements of the Public Records Act 2005.

The school principal should record the request, the information shared with the social worker, and the views of the learner (if it was practical and appropriate to consult with them).

Example – School requesting information from OT youth justice social worker

A school is preparing for a new learner due to start at the school after a period of time spent in a Youth Justice facility. The learner has been receiving education services whilst at the Youth Justice facility and is looking forward to returning to school. The school principal wants to know what the learner's charges and convictions were so that they can assess and identify any additional supports the learner may require.

Can the school principal request this information from the youth justice social worker?

Criminal offending history information is considered sensitive personal information. Misuse or unauthorised sharing of this type of information can be prejudicial to a learner and cause short- and long-term harm.

The school does not have an automatic right to the learner's criminal offending history. The school principal could request this information from the youth justice social worker using section 66C as the legal authority for the sharing of the information requested. As part of the request, the principal would need to provide the social worker with sufficient information to enable the social worker to be satisfied that the information was to be used for one of the purposes set out in section 66C – in this case completing an assessment of the learner's educational needs.

The responsibility for disclosing information under section 66C in this situation is on the social worker, including consulting with the learner. If the social worker doesn't reasonably believe that disclosing the information will assist the school in completing

the educational needs assessment, then they can refuse to provide the information requested.

When deciding whether to share sensitive information the best interests of the learner should always be considered. It would likely be in their best interests that the school is able to adequately support their reintegration back into school. In this case after considering whether sharing the criminal offending information is necessary for the purposes of the educational needs assessment, the potential prejudice and harm to the learner, and what would be in their best interests, the social worker could decide to advise the school principal that the charges and/or convictions were not of a nature where the learner may then require additional education support or would create a health and safety risk for the school, teachers or other learners.

Alternatively, the learner may consent to their criminal offending history, or certain parts of that history being disclosed (either by them directly or by the social worker) to the school for the specific purpose of identifying any additional supports that may require at school. Where the social worker was authorised by the learner to disclose the information, the legal authority for sharing the information with the school could also be the authorisation exception under IPP11 of the Privacy Act 2020.

Sharing under the Family Violence Act 2018 (when a learner is subject to family harm)

If you believe a child or young person is in immediate danger, call the Police on 111.

The following section provides guidance on how to share information under the Family Violence Act 2018.

You have a duty to consider sharing

Section 24 of the Family Violence Act requires that you actively consider sharing information about a victim or perpetrator of family violence to another FVA or SSP if you:

- believe on reasonable grounds that the sharing of information to that FVA or SSP will or may help ensure that a victim is protected from family violence
- receive a request from a FVA or SSP to share information for one or more of the purposes set out in section 20.

When you want or are asked to share (section 20)

Section 20 of the Family Violence Act 2018 permits the sharing of personal information when a child or young person is or has been subject to family harm.

Under section 20 you can proactively share information, or you can share information in response to a request.

Who you can share with

Section 20 of the Family Violence Act 2018 permits the sharing of personal information between Family Violence Agencies (FVAs) and Social Sector Practitioners (SSPs).

Family Violence Agencies (FVAs) are a group of organisations, and therefore their employees, or volunteers including:

- specified government agencies (see section 19, Family Violence Act 2018)
- non-government organisations funded by government to provide family violence-related services
- school boards and licenced early childhood education.

Schools and ECE services are FVAs under the Family Violence Act.

Social Sector Practitioners (SSPs) are professionals or people providing education, health or other social services including:

- teachers with current practising certificates
- registered health practitioners
- registered social workers.

A Charter School does not meet the definition of a Family Violence Agency under the Family Violence Act 2018. For the purposes of section 20, a Charter School is a Social Sector Practitioner.

Other agencies, organisations or individuals working within the education sector may also be a FVAs or SSP, but you should check to ensure you meet the definition of FVA or SSP under the Act before you share information for the purposes set out in section 20.

The purposes for which you can share

Section 20 enables sharing information about a learner who has been a victim of family violence where you reasonably believe that sharing the information will help the other FVA or SPP achieve one or more the following purposes:

- to help ensure that a victim is protected from family violence
- to make or contribute to a family violence risk or need assessment
- to make, or contribute to the making or carrying out of, a decision or plan relating or responding to family violence.

Section 20 enables sharing between any FVA and/or Social Services Practitioner e.g. between a school and a non-government organisation (NGO) that provides support to families experiencing family violence, between a ECE Service and a healthcare provider.

Section 20 permits sharing with a broader range of people than the serious threat exception under the Privacy Act. Under section 20 you can share with

any FVA or SSP who may be able to assist with identifying risk or providing support, whereas the serious threat exception under the Privacy Act will generally require disclosure to individuals with the power to intervene more directly.

If you receive a section 20 request for information and the purpose of the request is unclear, you should clarify the request with the requestor. If you are unsure why the information is being requested, you won't be able to determine whether one of the purposes set out in section 20 applies, or what information may be relevant to share with the requestor.

What information is relevant?

You can share information that you believe is relevant to help achieve one or more of the purposes set out in section 20. Deciding what information is relevant will often be a judgment call and depend on the circumstances of each situation.

Things to consider when deciding whether information is relevant include:

- your knowledge of the learner and their circumstances
- the person making the request, the purpose for which they are requesting the information and what they will be able to do with the information to support the learner and their family
- the age of the information – older information may be out of date and therefore less relevant to the current circumstances or needs of the child or young person.
- the context of the information – could the information be misinterpreted without additional context?

If you are unsure whether information you hold may be relevant, talk to the requestor or the person you want to share the information with. Together you may be able to identify what information is relevant in the circumstances.

Consent to share is not required

You **do not** need to obtain the consent of, or consult with, the learner (or their parents where appropriate) to share their information under section 20.

You should, however, consider the best interests of the learner – in some cases it may be in their best interests to let them know you are sharing their information, in other cases it could expose them to additional risk and harm.

Talking with the learner (or the parents where appropriate) can also help inform your decision about whether it is in their best interests to share their information in the circumstances.

Sharing in good faith

Sharing information under section 20 requires you to make a judgement call. Every circumstance will be different – in some cases you might decide to share, in others you might not. When you are under pressure, and a learner may be at risk, making these judgement calls can feel overwhelming.

The Family Violence Act provides protection from civil, criminal and disciplinary proceedings when you share information under section 20 unless you have shared in bad faith. Bad faith includes when you don't attempt to comply with the provision, or when you act carelessly or recklessly with information.

Acting in good faith means you have:

- made your best effort to share in line with the relevant statutory provisions
- checked that the information you intend to share is relevant, accurate, up to date complete and not misleading
- undertaken measures to ensure the information is shared safely with the right person in the right role.

You are protected from civil, criminal and disciplinary proceedings if you have shared information under section 20 unless you have shared in bad faith.

Confidentiality obligations

Obligations of confidence protect information deemed to be confidential from unauthorised access and disclosure. However, obligations of confidence are subject to exceptions which include situations where a child or young person's wellbeing or safety is at risk.

The Family Violence Act provides an exception to an obligation of confidence. The Act requires you to consider the principle that helping to ensure a victim is protected from family harm should usually take precedence over any applicable obligation to keep the information confidential.

However, you will need to ensure that:

- you are sharing for a purpose set out in section 20
- the confidential information is relevant to that purpose.

Helping to ensure a victim is protected from family violence is the guiding principle when sharing information under section 20. That principle should take precedence over any applicable duty to keep information confidential.

An individual staff member's professional code of ethics, industry code of conduct or employment agreement may set out what information is considered confidential and under what circumstances that information may be shared.

When advising a learner (or their parents where appropriate) that specific information, or categories of information, will be kept confidential you should always clearly inform them of the exceptions to that confidentiality i.e. the circumstances in which you may share that information.

For more information about privacy and confidentiality see: Chapter 4: Privacy and confidentiality.

When the requirements of section 20 aren't met

If you determine that the requirements of section 20 have not been met, you can consider whether one of the following applies in the circumstances:

- Section 66C of the Oranga Tamariki Act
- a Privacy Act IPP 11 exception.

Keep good records

It is important to keep good records of your information sharing activities. At a minimum you should record:

- the request you received and from whom (including receipt and response date)
- any additional information you requested from the requestor
- your decision whether, or not, to share the information requested
- the specified purpose you shared the information
- the information that you shared.

An easy way to do this is to create an Information Sharing Register. This can be as simple as an excel spreadsheet. Registers will contain personal information, and in some cases sensitive information. It is important to keep your information sharing Register secure (e.g. password protect your spreadsheet) and limit access to only those that need to have access.

How does the Privacy Act apply to sharing under the Family Violence Act 2018?

Section 20 authorises the sharing of personal information for specific purposes related to family violence. This means that you don't need to rely on one of the exceptions to Information Privacy Principle (IPP) 11 to share the information with another FVA or SSP.

However, you still need to comply with the other IPPs in the Privacy Act.

In practice, this means when you are **sharing** information under section 20 of the Family Violence Act, you must ensure you:

- share information in a safe and secure way and protect it from unauthorised access, use and disclosure (IPP5)
- have taken reasonable steps to ensure the information is accurate, up to date, relevant, complete and not misleading information (IPP8)
- are mindful about sharing unique identifiers (IPP13).

When you are **receiving** information requested or provided under section 20 of the Family Violence Act, you must ensure you:

- are requesting the information necessary for a lawful purpose of your agency (IPP1)
- meet your notification requirements (IPP3A after 1 May 2026)
- receive the information:
  - in a manner that is fair and not unreasonably intrusive on the child or young person's personal affairs (IPP4)
  - in a safe and secure way and protect it from unauthorised access, use and disclosure (IPP5)
  - only retain the information for as long as it is necessary to do so (Public Records Act and IPP9).

Learners (or their representatives) have the right to request access to and correction of their personal information under IPP6 and 7. If you correct personal information or attach a statement of correction to personal information that is also information that you have shared under the Family Violence Act, you must, so far as is reasonably practicable, inform that FVA or SSP of the correction.

Using the Family Violence Act in practice

The following examples work through the application of section 20 of the Family Violence Act.

Example – School Alerts Programme

Under the School Alerts programme schools can receive alerts about their learners who have been involved in a family harm episode in the last 24 hours. Names of the learners are provided to a participating school so they are aware of the incident, enabling them to identify and provide any additional supports learners may need while at school.

The legal authority for sharing the information with the participating school is section 20 of the Family Violence Act. The information is proactively shared to a school for the purpose of helping to ensure that a victim is protected from family violence. Section 20 also provides the legal authority for the school principal to share the information with a learner's teacher so that the teacher is aware and can contribute to the development of a support plan if one is required.

If a school requires further information about the learner and the family harm incident that occurred, it can use section 20 to request additional information from a relevant FVA or an SSP. The school must, however, be requesting the additional information for one of the purposes in section 20.

Example – ECE service (decision to share)

An ECE service manager receives a request for information about a learner enrolled in its service from a local organisation which provides support to families who are or have experienced or family harm. The organisation has requested information about the learner to help them developed a comprehensive support plan for them and their

family. The information requested includes attendance, behaviour, and any incidents that have occurred at the ECE that may be relevant to the development of that plan.

Can the ECE provide the information to the requesting organisation?

To use on section 20, both the ECE service manager and the requesting organisation must be either a Family Violence Agency (FVA) or a Social Services Practitioner (SSP). Under the Family Violence Act a licenced ECE service is a FVA. To be a FVA, the requesting organisation must be a non-governmental organisation that is wholly or partly funded by government to provide family harm services. The ECE service manager should check with the requesting organisation that they are a FVA or the person making the request is a SSP.

The information being requested is for one of the purposes set out in section 20 (making a support plan for the family who have experienced family harm) and is relevant to achieving that purpose. The information will help the requesting organisation to ensure that the child and their family get appropriate and effective supports including those which ensure the child can attend the ECE service. It would be appropriate for the ECE service manager to rely on section 20 to share the information with the requesting organisation (once they have confirmed the requesting organisation is a FVA or SSP).

While section 20 provides the legal authority to share the information, the ECE service manager must still comply with IPP1 and 4 (lawful purpose for collection, necessity, method of collection), IPP5 (security and storage), IPP6 and 7 (access and correction rights), IPP8 (accuracy) IPP9 (retention of information) and IPP13 (unique identifiers) requirements.

The ECE service manager should record details of the request including the request, what was shared and for what purpose.

When you are required to share information

Legislation may require you to share personal information for specific purposes. Some examples of these types of legislative provisions include:

- section 17B of the Tax Administration Act 1994
- section 66 of the Oranga Tamariki Act 1989
- section 23 of the Data and Statistics Act 2022
- section 619 of the Education and Training Act 2020
- section 22 of the Education and Training Act 2020
- schedule 6 clause 2 of the Social Security Act 2018
- section 27 of the Children's Commissioner Act 2022
- schedule 5 of the Pae Ora (Healthy Futures) Act 2022
- section 20 of the Inquiries Act 2013

When a government agency uses a legislative provision requiring you to provide information they should provide you with a notice. A notice requiring the provision of information:

- should be made by the government agency in any prescribed form that might apply
- clearly identify the legal authority under which the notice has been issued
- clearly state the information you are required to provide and for what purposes.

When you receive a notice, you **must** provide the information requested to the issuing agency within the specified timeframe. You should also record the notice and your response to the notice in your information sharing register.

Example – Mortality Review Committee requesting information

You have received a request for information about a number of individuals from the chairperson of a Mortality Review Committee. The request is for personal information, including health information about the individuals listed in the request.

Can you share this information with the chairperson?

Yes, you can. Mortality Review Committees are set up under the Pae Ora (Healthy Futures) Act 2022, and Schedule 5 of that Act grants the Mortality Review Committee (or the appointed agent) the power to source any information relevant to their purpose.

Given the sensitive nature of the information, make sure that you share the information using a secure method to protect the personal information.

Example – Request from Ministry of Education to a school

As the chairperson of the school board, you have received a request from the Ministry of Education for information about learners who participated in a Ministry funded literacy programme. The request includes personal information about the learners including their name, year level, whether they completed the programme and whether participation in the programme resulted in literacy improvements. The information will be used by the Ministry for reporting (statistical) purposes.

Can you share this information with the Ministry?

Yes, you can. The Ministry of Education has powers under section 619 of the Education and Training Act to request information from a school board for the purposes of administering the Act. Under these powers, the Ministry can request personal information about learners for statistical purposes.

Given the potentially sensitive nature of the information, make sure that you share the information using a secure method to protect the personal information.

Example — Request for information from an OT care and protection co-ordinator

You have received a request for information about a learner from an Oranga Tamariki care and protection coordinator. The information is required for the purposes of a family group conference.

Can you share this information with the requestor?

Yes, you can. Oranga Tamariki have the powers under section 66 of the Oranga Tamariki Act to request information for specified purposes, including the facilitation of a family group conference.

Given the sensitive nature of the information, make sure that you share the information using a secure method to protect the personal information.

Information sharing in practice

The following section works through common information sharing examples in the education sector.

Sharing with other education providers

Enrolment records - Schools

The Education and Training Act (section 237(2)) provides legal authority for sharing enrolment records between registered schools.

When a learner has enrolled in a new school, the principal of the old school must ensure that the learner's enrolment records are shared with the principal of the new school – you do not need to consider whether an IPP11 exception or other legal authority applies.

Enrolment records are defined in the Rules for Student Enrolment Records Gazette Notice: Rules for Student Enrolment Records - 2007-go7062- New Zealand Gazette.

ENROL is the system used to capture enrolment records for all learners. Schools are required to use ENROL unless they have received an exception from MoE. ENROL enables enrolment records to be shared between schools. When a learner enrols in and moves to a new school, the new school will have access to the learner's enrolment record via ENROL.

This specific legal authority under the Education and Training Act applies only to enrolment records. This means that **no** other information about the learner e.g. attendance or learning support information should be shared with the **new school** unless:

- another provision of the Education and Training Act (e.g. directed enrolment) applies
  or
- an IPP11 exception applies
  or
- another legal authority applies.

Example – Learner transferring to new school

A learner has enrolled in a new school. The new school has received the learner's enrolment application and is currently processing the application.

The enrolment form collects information about any learning support needs the learner may have to help them ensure they have appropriate supports and resourcing available to support the learner. The learner's parents have noted in the enrolment form that their child has learning support needs but has not provided any details about what those needs are. The parents have not ticked the box consenting to the new school obtaining the learner's learning support information from the learner's current school.

The principal of the new school emails the principal of the current school asking for the learner's learning support information.

Can the principal of the current school share this information?

No, they can't. Learning support information is not part of a learner's enrolment record under the Rules for Student Enrolment Records. The learner, or their parents, need to consent to the learning support information being shared with the new school. In this case, the parents have not explicitly provided consent. The principal of the new school should contact the parents and either seek the information from the parents directly or obtain consent for the information to be shared by the current school.

Enrolment records - ECE services

When a learner moves to a new ECE, the new ECE will have access to the learner's enrolment record via ELI. ELI is the system used to capture enrolment records for all learners. ECEs are required to use ELI unless they have received an exception from MoE

This means that **no** other information about the learner, outside of that contained in ELI, should be shared with the new ECE unless the learner or their parents has consented to that information being shared.

Example – Learner transferring to new ECE

A learner has enrolled in a new ECE. The new ECE has received the learner's enrolment application and is currently processing the application.

The enrolment form collects information about any learning support needs the learner may have to help them ensure they have appropriate supports and resourcing available to support the learner. The learner's parents have noted in the

enrolment form that their child has learning support needs but has not provided any details about what those needs are. The parents have not ticked the box consenting to the new ECE obtaining the learner's learning support information from the ECE the learner is currently attending.

The manager of the new ECE emails the manager of the current ECE asking for the learner's learning support information.

Can the current ECE manager share this information?

No, they can't. Learning support information is not part of a learner's record in ELI. The learner, or their parents, need to consent to the learning support information being shared with the new ECE. In this case, the parents have not explicitly provided consent. The ECE manager of the new ECE should contact the parents and either seek the information from the parents directly or obtain consent for the information to be shared by the ECE their child is currently attending.

Dual Tuition or Enrolment

In some cases, a learner may have dual tuition or enrolment.

Information about the learner will often need to be shared to facilitate dual tuition or enrolment. In most cases, information shared for this purpose should be with the consent of the learner or their parent. It is important to ensure that only information **necessary** for the purpose of referring and assessing and approving dual tuition or enrolment should be shared.

Where a learner has dual tuition or enrolment, the education provider at which the learner is enrolled retains all legislative accountabilities, including those under the Privacy Act. The education provider providing the additional education service is also accountable for ensuring the learner's personal information they collect, use and share is managed according to the Privacy Act.

All other learner information

Sharing of any other learner information with education providers must have a legal authority that permits the sharing. For example:

- An IPP11 exception.
- Section 66C of the Oranga Tamariki Act.
- Section 20 of the Family Violence Act.
- Other legislation such as the Education and Training Act.
- An information sharing provision that requires specified information to be shared for a specified purpose.

Example – School roll planning

A secondary school is planning for new enrolments the following year. The principal sends an email to all intermediate and composite primary schools in the local area asking them to provide a list of their learners in year 8. The principal advises that this information will be used for school resourcing planning.

Can the principals of the intermediate and composite primary schools share this information?

No, they can't. Unless the learners or their parents have consented to this information being shared there is no legal authority permitting this sharing of information about learners. Additionally, not all year 8 learners will be enrolling in that specific secondary school, so the secondary school will be collecting information that is not necessary to achieve the intended purpose.

Example – learning support registers

A primary school is part of a group of schools and ECE services (cluster) that work together to share resources. A primary focus for the cluster is timely provision of learning support services. Each school and ECE service has a learning support

register. These registers document the learners who are require additional learning supports, what learning supports they are receiving and by whom.

The cluster group wants to share their learning support registers and create a cluster level register. The cluster level register will be used to help manage learning support resources effectively across the cluster.

Can each school and ECE service within the cluster share their learning support register for this purpose?

Each school and ECE service **must** obtain the consent (IPP11 authorisation exception) of the learner or their parents for the learning support information to be shared with the other schools and ECE services in the cluster for the intended purpose. Even after consent is obtained, only learning support information that is relevant to the purpose of allocating learning support resources effectively should be shared – it may not be necessary to share all information contained in the school or ECE service level register.

Learning support registers will likely contain sensitive information about learners. Access to these registers should be restricted to staff that need to know and are in a position to use the information for the intended purposes.

Sharing within an education provider

Information sharing isn't just about sharing a learner's personal information externally. It also occurs internally within your organisation e.g. a conversation or email between teachers about a learner, a list of learners and their learning support needs place on a notice board in the staff room.

The Privacy Act refers to this kind of internal sharing as a "use" of information within your organisation, rather than a "disclosure". As well as considering whether the use of a learner's information is permitted under IPP10, when sharing internally you

should always consider who in your organisation actually needs to know that information.

Example – Staff Meetings

A primary school teacher has received information from one of their learner's parents that the learner's parents are separating and the learner is struggling with the separation. The parent advises the teacher that the separation is amicable, and both parents want to ensure that their child is supported through this time. The parent has advised that they don't mind relevant staff being advised of the separation, but do not want the information shared widely at this stage.

Can the teacher share this information with other teachers at the weekly staff meeting?

Information about the learner's family situation is sensitive information so the teacher should be mindful about who they share the information with and for what purpose. While the parent has consented to sharing information about the separation, they have asked that the information is only shared with relevant staff.

Not all school staff engage with the learner on a daily basis, so it wouldn't be appropriate to share the information at the weekly staff meeting. The teacher could, however, arrange a smaller meeting with staff that do engage with the learner regularly (for example, school sport coaches, kapa haka coach, the principal, and the guidance counsellor) and let them know about the separation, that the learner is struggling with it, and to be aware that the learner may require additional support during this time.

Teachers and staff receive a lot of information about learners on a day-to-day basis. Some of this information may need to be shared to ensure the wellbeing and safety of learners and ensure they are getting the learning supports or services they need.

However, staff meetings may not always be the appropriate place to share information, particularly sensitive information such as health or medical conditions or family circumstances. Not everyone present at a staff meeting will need to know and will not be in a position to do anything with the information. Think carefully about whether a general staff meeting is the most appropriate place to share information about a learner, a smaller more learner focused meeting may be more appropriate.

Education provider sharing with service providers

Where a learner requires additional support (e.g. health, social or cultural supports) a school or ECE service may need to engage a service provider (e.g. a non-government organisation, marae-based services or a private business) to assist.

The education provider may need to share information about the learner with the service provider to:

- make a referral

  and
- support the service provider to identify, deliver and assess the effectiveness of the services provided to the learner.

Referrals

When a school or ECE service refers a learner to a service provider they should obtain the consent of the learner or their parent to make the referral. When making the referral, you should only share information that is necessary for the service provider to assess and approve the referral should be provided.

As part of the consent process, the learner or their parent should be advised why the referral is being made, to whom the referral is being made, and what the service provider will do with the information. This enables the learner or their parent to make

an informed decision to consent to the referral being made, and the for the information to be provided to the service provider.

Where consent is provided to make the referral, the information must be provided to the service provider in a safe and secure way.

Information to support delivery of services

Service providers

When a referral has been accepted by the service provider it may be necessary for them to seek more detailed information about the learner to identify and deliver appropriate services. The service provider may also need information to help them assess the effectiveness of the services being delivered.

When a service provider requests (collects) information about the learner it must ensure that it is collecting the information appropriately (see Chapter 5: Collecting Information).

Education providers

When responding to a request from a service provider, the education provider should make sure they know the legal basis for which the information is being requested. For example:

- Has the learner or parent provided consent for the information to be provided by the school or ECE service?
- Is the request being made under another information sharing provision such as section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act?

If you are unsure, you should seek clarification from the service provider before you share information with them.

When you are satisfied that a legal authority exists to share the information, you must ensure that the information you are sharing is accurate and up to date (IPP8),

and the information must be provided to the service provider in a safe and secure way (IPP5).

Sharing with parents

Section 165: Education and Training Act 2020 – Monitoring of and reporting on student performance

A school board must ensure that information about a learner's performance is shared with that learner's parents in a timely manner and in a form that is easily understandable.

If section 165 is used as the legal authority to share information with a parent, the school board **does not** need to consider whether an IPP11 exception or other legal authority applies. However, the school board must ensure that the information shared is accurate (IPP8) and is provided to the parents in a secure way (IPP5).

Section 103: Education and Training Act 2020 – State and Charter schools

State, state integrated and charter schools must inform parents of matters that, in the opinion of the state school principal or person responsible for teaching and learning at a charter school are:

- preventing or slowing the learner's progress through the school

  or
- harming the learner's relationships with teachers or other students.

It is up to the state or state integrated school principal or the person responsible for teaching and learning at a charter school to determine, in the circumstances, what learner information is relevant to the two purposes above and should then be shared with the parent.

If the section 103 is used as the legal authority to share information with a parent, the state or state integrated school or charter school **does not** need to consider

whether an IPP11 exception or other legal authority applies. However, the state or state integrated school principal or the person responsible for teaching and learning at a charter school must ensure that the information shared is accurate (IPP8) and is provided to the parents in a secure way (IPP5).

Requests for information from parents

The Privacy Act does not provide parents with an automatic right to information about their children.

If you receive a request for information from a parent and the information requested is not covered by sections 103 or 165 of the Education and Training Act, you will need to determine whether the parent is acting as a **representative** of the learner and exercising the learner's access (IPP6) and correction (IPP7) rights under the Privacy Act on their behalf.

For more detailed guidance on how to respond to a request for information about a child or young person see: Office of the Privacy Commissioner | Responding to requests for a child or young person's personal information.

Sharing in emergencies

State of national emergency

The Civil Defence National Emergencies (Information Sharing Code) 2020 (the Code) enables agencies to collect, use and share personal information in the event of a major disaster that has triggered a state of national emergency.

The Code facilitates the sharing of information to:

- relevant agencies to assist the government response to the national emergency, and
- a person who is responsible for an individual who may be involved in the emergency (e.g. the parent or other relative of a learner).

For an education provider, this means that when a state of national emergency is declared, you can share personal information about learners with a public sector agency, or an agency involved in managing or assisting with the emergency for permitted purposes.

For example:

- The education provider could share the names and other relevant information about learners who are at a school and are unable to return home due to the emergency with Police.
- The education provider could share health information about learners with medical conditions who are not able to return home due to the emergency with a health care provider.

For more information about the Code see: Office of the Privacy Commissioner | Civil Defence National Emergencies (Information Sharing) Code 2020.

Traumatic events

Traumatic events are sudden, unpredictable events that can occur with no warning. Traumatic events are those that:

- Cause sudden and/or significant disruption to the operation of an education provider.
- Have potential to affect a large number of learners and staff.
- Create significant dangers to the physical and emotional wellbeing of learners, staff and the wider community.
- Often attract media attention.

Examples of traumatic events include:

- A sudden accidental or non-accidental death or serious injury of a learner, their family member or a staff member

- Witnessing serious injury or death of a learner, their family member or a staff member.
- Threats to the safety of learners or staff.
- A missing learner or staff member.
- Floods, fires, earthquakes or other community crisis or natural disaster.

Managing a traumatic event can be stressful with many moving parts. You will be receiving a lot of information from various people, and there will often be gaps in information about what is happening. Learners, their parents and staff will be wanting information to understand what is happening. Knowing what you can and shouldn't share during a traumatic event can help ensure such events are managed effectively.

Sharing information about learners

Depending on the nature of the traumatic event you may be asked to share information about learners from agencies or organisations responding to the event.

Where there is a serious threat to the life or health of the learners, you can consider whether sharing relevant learner information under the IPP11 serious threat exception is appropriate in the circumstances.

For example:

- You may need to share learners' health information with medical responders to help ensure learners with urgent medical needs are triaged and assisted appropriately.
- You may need to share information about learners to help public health officials prevent and manage an outbreak of an infectious disease in the community.

Where you have concerns for the wellbeing or safety of your learners and risk or needs assessments of the learners are necessary, you can consider whether sharing relevant learner information under section 66C of the Oranga Tamariki Act is appropriate in the circumstances.

For example, you may need to share information about learners with specialist trauma counsellors to ensure they get appropriate support during and after the traumatic event.

Where a traumatic event is about a learner, information about them and the circumstances of the event should not be shared unless:

- You are sharing the information to support Police, or another law enforcement agency, investigate the event (IPP11 law enforcement exception).
- You are sharing the information to support a coronial inquiry.
- You have the consent of the learner's parents to share specific information about the learner and the event (IPP11 authorisation exception).

Extra care should be taken with information about allegations of criminal offending or abuse. Sharing this type of information could significantly impact the learner concerned and their family and impede any criminal investigation that may be underway.

Sharing with education agencies

The Education and Training Act 2020 and associated regulations provide the legal basis for sharing learner information with education agencies for specified purposes.

Education agencies include:

- Ministry of Education (MoE).
- New Zealand Qualifications Authority (NZQA).
- Education Review Office (ERO).

- Teaching Council New Zealand Aotearoa (TCNZ).

Where the Education and Training Act provides a legal authority for sharing information, you **do not** need to consider IPP11 or other information sharing provisions (e.g. Oranga Tamariki Act or Family Violence Act).

You still need to ensure that the information you are sharing with an education agency is shared safely and securely and is accurate and up to date.

You will need to let your learners (and their parents where appropriate) know what information you share with education agencies, the legal basis for sharing the information and how the information is used by those agencies. An easy way to do this is to document your information sharing with education agencies in your privacy policy.

Sharing with the Ministry of Education (MoE)

Schools

The Education and Training Act (section 619) enables MoE to collect information about learners directly from schools for certain purposes (e.g. statistical purposes, ensuring learners and education providers receive appropriate funding or enrolment and attendance purposes).

Where MoE is using its powers under the Education and Training Act, it does not require the consent of learners or their parents to collect this information.

MoE collects this information in a number of ways, including:

- enrolment information entered in ENROL and ELI
- attendance data collections
- School Roll Returns
- ECE Service Census Returns.

MoE uses the learner information to fulfil its functions under the Education and Training Act which include funding and staffing schools, policy analysis and development, monitor outcomes of the education system, undertaking research and publishing education statistics and identifying learners that may require additional learning support.

Where schools are required to provide learner information to MoE, you do not need to consider whether an IPP11 exception or other legal authority (e.g. Oranga Tamariki Act or Family Violence Act) applies.

Because schools have initially collected the information directly from the learner or their parents (at enrolment or throughout the learner's education journey), the school is required to comply with IPP3 and inform the learner or their parents:

- that learner information collected by the school will be shared with MoE to enable MoE to fulfil its functions under the Education and Training Act
- what learner information is being shared
- how MoE will use the learner information
- how it is being shared and kept safe
- the learner's rights to access (IPP 6) and correct (IPP 7) their information.

For more detailed information about the School Roll Return process see: School Roll Return Guidelines | Education Counts.

Outside of enrolment records, attendance data collections, and School Roll Returns MoE may request learner information from a school for other purposes. Such situations may include when MoE is:

- assessing a learner's eligibility for services or funding offered by MoE
- undertaking an evaluation of education services and programmes
- undertaking a specific research project
- seeking confirmation of how funding was utilised.

Where the information being shared with MoE is not for one of the purposes set out in the Education and Training Act, the school should ensure that a legal authority exists for sharing the information with MoE (e.g. an IPP11 exception or another legal authority such as those under the Oranga Tamariki Act or Family Violence Act).

The school should also consider whether MoE already hold the information that is being requested about a learner or group of learners. Where MoE already holds the information, then the school can consider whether it is appropriate to decline the request.

ECE Services

ECE services must comply with minimum requirements set out in the Education and Training Act and Education (Early Childhood Services) Regulations 2008 and the Education (Playgroups) Regulations 2008.

The Education and Training Act (section 22) requires licenced ECE services to keep and make available to MoE specified records. Information that MoE requires licenced ECE services to provide includes:

- a register of the children who attend or have attended the service, specifying the date of birth of each
- a record of the attendance of children at the service
- a record of all fees and other charges paid in respect of children's attendance at the service
- evidence that parents of children attending the service have regularly examined the attendance record
- any other records that are necessary to enable the service's performance to be monitored adequately.

This information is shared with MoE using the Early Learning Information System (ELI).

For more detailed information on ELI and its privacy related requirements see: Early Learning Information (ELI) and Privacy and ELI Principles of Use | Applications & Online Systems.

ECE services and certificated playgroups must also ensure that appropriate written procedures and records are developed and maintained and made available upon request by any person exercising powers or carrying out functions under section 626 (powers of entry and inspection without warrant) of the Education and Training Act.

Where an ECE service or certificated playgroup is sharing information under the requirements of the Education and Training Act and associated regulations, they do not need to consider whether an IPP11 exception or other legal authority applies.

Sharing with New Zealand Qualifications Authority (NZQA)

NZQA are responsible for managing the New Zealand Qualifications and Credentials Framework, running the assessment system for secondary schools, and keeping complete records of learners' educational achievements.

The Education and Training Act (section 458) provides NZQA with the powers to collect information to carry out its functions.

Secondary schools are required to share learner information to NZQA for the purposes of assessment and issuing of qualifications. Information shared includes the learners name, National Student Number (NSN), residential address, the standard and assessment information and the name of the school.

For more information on sharing learner information with NZQA see: Managing school data - NZQA.

Sharing with Education Review Office (ERO)

ERO is an external education review agency. ERO is responsible for evaluating and reporting on the education of learners by education providers.

The Education and Training Act (section 464) provides ERO with the powers to collect information to carry out its functions. Those functions include reviewing, inspecting and reporting on the performance of education providers.

When exercising its information collection powers, ERO makes it clear that it does not collect personal information about learners as part of its review process. When responding to a request for information ensure you are not providing personal information about your learners (e.g. redact learners names from reports or documents).

Sharing with Teaching Council Aotearoa New Zealand

The Teaching Council is the professional body for registered and certificated teachers across early childhood, primary and secondary education in both English and Māori medium settings. The functions of the Teaching Council are set out in the Education and Training Act 2020. These functions include performing the disciplinary functions relating to teacher misconduct and reports of teacher convictions and performing the functions relating to teacher competence.

To perform this function, the Teaching Council will often require information from schools and early childhood services to assess and investigate reports and complaints about teacher conduct or competence.

Under the Education and Training Act 2020 (Part 5, Subpart 4), the Teaching Council may request information to be provided within a specified timeframe from:

- school boards
- a service provider that operates any licenced early childhood service or any certified playgroup
- managers of a private school.

The requirement to provide this information is dependent on the stage of the disciplinary process that the matter is at.

In all cases, the Teaching Council will make clear what legislation they are relying on to request the information so that you can make an informed decision on the appropriate action.

Triage

When a report or complaint is first received by the Teaching Council, the Triage Committee completes an initial assessment of the matter and determines whether further action is warranted. Under rule 11C(2)(a)(i) of the Teaching Council Rules 2016 the Triage Committee may request further information from any person.

These requests are different to the ones made under sections 497(7), 502(1)(b) and 507(2) of the Education and Training Act 2020, detailed further below, and you are not obliged to provide information at this stage. In this case, you should consider whether an IPP11 exception under the Privacy Act applies.

You also need to ensure that you provide relevant and up to date information (IPP8) and that you supply the information to Teaching Council in a secure manner (IPP5).

Complaints Assessment Committee (CAC)

Section 497(7) of the Education and Training Act 2020 and rule 15(3) of the Teaching Council Rules 2016 provide the CAC, and investigators appointed to conduct investigations on behalf of the CAC, the power to require an employer, former employer, or a government agency to provide information necessary for the purposes of an investigation.

You still need to ensure that you provide relevant and up to date information (IPP8) and that you supply the information to the Teaching Council in a secure manner (IPP5).

New Zealand Teachers Disciplinary Tribunal (DT)

Section 502(1)(b) of the Education and Training Act 2020 provides the DT with the power to require a person to produce any documents, records, or other information that relate to the subject matter of the hearing.

You still need to ensure that you provide relevant and up to date information (IPP8) and that you supply the information to the Teaching Council in a secure manner (IPP5).

Competence Authority (CA)

Section 507(2) of the Education and Training Act 2020 states that the Teaching Council may require the teacher's current or former employer to supply information for the purpose of investigating a report that relates to the teacher's competence. Under this section, the current and/or former employer must supply this information.

You still need to ensure that you provide relevant and up to date information (IPP8) and that you supply the information to the Teaching Council in a secure manner (IPP5).

Sharing at multi-agency meetings

A multi-agency meeting is a meeting where different agencies and organisations come together for a common purpose e.g. identifying effective supports for learners who are not regularly attending school.

Sharing information about learners in such settings often an effective and efficient way to identify appropriate supports, interventions and services in a collaborative and timely manner.

You need to ensure, however, that you:

- have a legal authority to share the information (e.g. section 66C of the Oranga Tamariki Act, section 20 of the Family Violence Act, or an IPP11 exception),
- are sharing relevant information about the learner or their family and whānau
- are sharing that information with the right people
- record your information sharing activities.

To be confident you are sharing learner information appropriately you need to embed best practice information sharing into the governance and operation of your multi-agency meetings. This will protect the learners you are sharing information about and help you meet the objectives of your multi-agency meetings in a privacy protective and respectful way.

For more guidance on how to set up good information sharing practice for your multi-agency meetings see: Sharing information at multi-agency meetings.

Keeping learners and parents informed

Being transparent about how you collect, use, and share personal information is a requirement of the Privacy Act.

Transparency also helps you build trust and confidence in the way your organisation manages personal information. It also helps ensure learners are aware of their privacy rights and how they can exercise those rights.

Informing learners (or their parents where appropriate) about collecting their information is not a 'one and done' thing. Each time you collect personal information you need to think about how you inform them and what that communication should look like.

Relevant information privacy principles

The Privacy Act 2020 sets rules about when and how an education provider is required to inform learners when collecting their personal information.

The relevant information privacy principles (IPPs) are:

Principle 3: Collection of information from an individual

When an education provider collects personal information directly from a learner you must take steps that are reasonable in the circumstances to inform the learner of:

- the fact that information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information
- the name and address of the education provider collecting and holding the information

- if the collection of information is required by law, the particular law under which the information is required, and whether the supply of information is voluntary or mandatory
- the consequences, if any, of not supplying the information
- the rights of access to and correction of the information supplied.

Principle 3A: Indirect collection (applicable from 1 May 2026)

When an education provider collects personal information from someone other than the learner (e.g. their parents or another person), you must take steps that are reasonable in the circumstances to inform the learner of:

- the fact that information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information
- the name and address of the education provider collecting and holding the information
- if the collection of information is required by law, the particular law under which the information is required
- the rights of access to and correction of the information supplied.

When do the notification requirements apply?

IPP3 applies when you collect personal information directly from a learner.

Being transparent about your collections builds trust. If you are transparent about how you manage a learner's personal information, then they will be more likely to share their information with you.

The reality is that education providers collect a significant amount of personal information about learners from their parents (or guardians) under exceptions to IPP2. This means that the requirements of IPP3 won't apply where you have

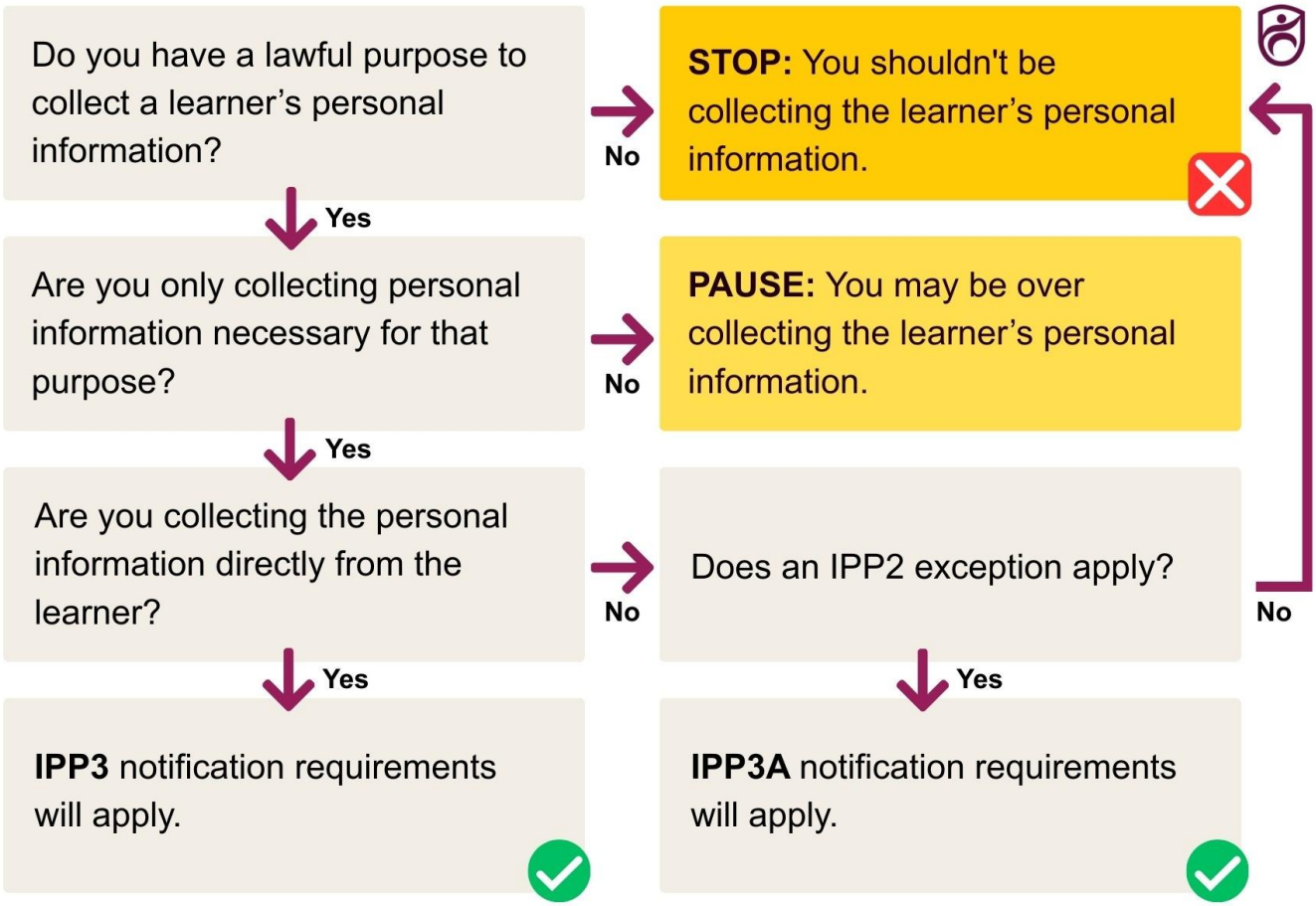
collected a learner's personal information from their parent or guardian or someone else.

For more information about IPP2 and whether an exception applies see Chapter 5: Collecting Information.

IPP3A applies when you collect personal information about a learner from someone else (e.g. a learner's parent, legal guardian).

For more detailed information about IPP3A see our guidance: Office of the Privacy Commissioner | IPP3A: notification requirements for indirect collection of personal information.

When IPP3 and IPP3A applies: Flow Chart



Flowchart for determining how IPP3 and IPP3A applies to collection of personal information.

How to inform learners and parents

IPP3 and IPP3A require that you inform the individual whose information you are collecting about the collection. However, in the education sector this may not be straightforward due to the age and capacity of your learners, and the fact that in many cases you will be collecting information about your learners from their parents.

IPP3 and IPP3A require education providers to take all steps, that are reasonable in the circumstances, to ensure a learner is aware that the information is being collected. For younger learners, or learners that don't have the ability to fully understand, informing the learners' parents would be a reasonable step for you to take to ensure this requirement is met.

For your older learners, some may not be able to fully understand what the notification requirements of IPP3 and IPP3A mean for them and their personal information. Therefore, in those circumstances, it would be a reasonable step to inform the learner's parents so that they can help make sure the learner fully understands the purpose of the collection, whether they have to provide the information or not, and their rights to access and correct that information.

In some cases, you will be collecting personal information about the learner and their parents e.g. information collected from parents through the enrolment process. When this occurs:

- IPP3 requirements will apply to the collection of information about the parents **and**
- IPP3A requirements will apply to the information about the learner.

What to tell learners and parents

The following sections break down the requirements of IPP3 and IPP3A and help you work through the things you should think about to ensure you are informing learners (or their parents where appropriate) appropriately.

Purpose

You must have a lawful purpose for collecting personal information about a learner **and** the information you are collecting must be reasonably necessary for you to achieve that purpose.

IPP3 and IPP3A require you to inform learners (and their parents where appropriate) about why you are collecting their personal information e.g. the purpose of collection.

Learners (and their parents where appropriate) should be able to easily understand what information you are collecting, why you are collecting it and what you are going to use it for.

Parent example - Health form - Medication information for primary school camp

We are collecting information about medication requirements your child may have to ensure they receive their medications appropriately and to help us effectively manage your child's health and wellbeing while they are attending our school camp.

We collect this information to ensure we meet our obligations under the Education and Training Act 2020, the Health and Safety at Work Act 2015, the Children's Act 2014 and other relevant legislation.

Information Required: Information about any medications your child will need to take, whether your child requires assistance to take their medication(s) and what this assistance involves, and any relevant information about the medical condition we

need to be aware of to manage your child's health and wellbeing appropriately while at the school camp.

The information you provide about your child will only be used for the specified purpose above.

Learner example - Term 1 In-class orientation survey for year 9 learners

Purpose statement: The first term at secondary school can feel a bit scary. There are a lot of new things to learn, and a new school environment to get used to. The purpose of this wellbeing survey is help us (your teachers) make sure you are settling in well and know where you can go to get help and assistance if you need it. It also helps us to make sure our orientation activities are helpful to learners beginning their secondary school journey.

Information Required: Your name, your thoughts on our orientation activities, your ideas about how we could improve those activities, and whether you would like or need further support or help settling in.

For more information about collecting personal information, including developing good purpose statements, see Chapter 5: Collecting Personal Information.

Intended recipients

You must inform learners (or their parents where appropriate) who will have access to the information you are collecting and how they will use it. This includes information about an organisation that may be collecting the information on your behalf, and other organisations that you may share the information with and why.

Parent example - Health form - Medication information for primary school camp

Who we may share your child's information with: Your child's medications information will be shared with our Camp Managers so that they are aware and informed and can assist your child appropriately if required. In the case of a medical event, we may need to share your child's health information with healthcare providers to ensure appropriate medical assistance is provided.

Learner example - In-class survey

The information you provide in this survey will be seen by your teacher. Your feedback about the orientation activities will be provided to the principal and other school staff. Don't worry though, they won't be told who provided the feedback. If you have requested additional support or help settling in, your teacher will share your name with the appropriate person who can help you.

For more information about sharing personal information see Chapter 7: Sharing Personal Information.

Authorised or required by law

IPP3 and IPP3A require you to inform learners (or their parents where appropriate) whether the collection of their personal information is authorised or required by law.

Where the collection is authorised or required by law and you are collecting that information directly from the learner, you must also inform the learner (or their parents where appropriate) whether the provision of the requested information is mandatory or voluntary.

Example - Collection of learner information required by law

The Education and Training Act 2020 requires schools and ECE services to collect specified information about learners at the time of enrolment i.e. the collection of this information is required by law.

Learners (and their parents where appropriate) should be informed that:

- the collection is required by the Education and Training Act 2020
- the information that the school or ECE services is required to collect
- what that information will be used for and who it may be shared with
- whether the provision of information requested is mandatory or voluntary
- any consequences of not providing the mandatory information

The learner's right to request access to and correction of their personal information including the process by which they can make those requests.

For more information about mandatory information requirements under the Education and Training Act see Enrolment section later in this chapter.

Consequences if information isn't provided

When you are collecting information directly from a leaner, you must also inform the learner (or their parents where appropriate) of any consequences of not providing the information (e.g. enrolment won't be progressed, funding for a service may not be available, the learner may not be able to participate in an activity).

Access and correction rights

Learners (and their parents where appropriate) must be advised of their access (IPP6) and correction rights (IPP7) under the Privacy Act. You must inform a learner (or their parents where appropriate):

- that they can request access to, or correction of, the personal information at anytime

  and
- the process by which they can make an access or correction request.

Parent example - Health form - Medication information for primary school camp

Your rights and how you can exercise them: As your child's representative, you can exercise your child's right to request access to and correction of the personal information we are collecting from you.

You can make an access or correction request on behalf of your child by emailing [insert email address] or contacting us by phone [insert phone number].

Learner Example - In-class survey

You can always ask to see any personal information that the school holds about you. You can also ask us to correct any information that is wrong. Just ask your teacher and they will help you.

For more information about managing access and correction requests see Chapter 13: Managing requests for information.

When do I need to inform learners/parents?

You should always try to inform them **before** you collect their personal information.

If that is not possible, then you need to inform them as soon as practicable after the information is collected.

When you aren't required to inform learners and parents

There are some situations where you don't need to inform a learner (or their parents where appropriate) about the collection of their information. IPP3 and IPP3A exceptions relevant to the education sector include:

- if you have recently informed the learner of the same collection, of the same information or information of the same kind
- if you reasonably believe that not informing the learner would not prejudice their interests
- that compliance would prejudice the purposes of the collection
- that compliance is not reasonably practicable in the circumstances
- that the information being collected will not be used in a form where the learner can be identified
- that the information being collected will be used for statistical or research purposes and will be published in a form where the learner isn't identified.

Example - Recently informed learner of collection

A school runs an in-class survey each month asking learners in years 10 – 13 to provide feedback on the lunches provided by the school. When the survey was first introduced, the school principal informed the learners about the purpose of the survey covering all the requirements of IPP3.

Does the school principal need to notify the learners every time the survey is completed?

As the learners have already been informed about the survey and the survey collects the same information from the same students each month, the school principal does not need to notify the learners each time. However, as the survey is voluntary and some learners may not complete the survey regularly it is good practice to make sure the learners know where they can go to get information about the survey.

Age-appropriate communication

When you are collecting information from learners (e.g. through an in-class learner wellbeing survey) you need to ensure that you are informing them about the collection of their personal information and how it will be used, in a way that they will understand.

This may mean you need to develop different communication content and delivery methods for learners of different ages and abilities.

If your learners don't understand what information is being collected, why it is being collected and how it will be used, the means of collection could be considered unfair.

For more information about method of collection see Chapter 5: Collecting Information.

Example - Informing a learner when undertaking disciplinary investigations

When investigating an allegation of learner misconduct, you will be collecting personal information about the learner– for example, what they did, when they did it, who they were with, what they saw, what they heard, or why they may have done or not done something.

Disciplinary processes are a stressful time for all involved, especially for a learner. IPP4 requires you to take extra care when collecting information from learners and ensure the way in which you collect their information is fair and doesn't intrude to an unreasonable extent into their personal affairs. Making sure the learner (or their parents where appropriate) understands why you are collecting their information and how it will be used in the investigation process helps to ensure the way you are collecting the information is fair.

When collecting information from a learner as part of an investigation process things you should consider include:

- Is the learner of sufficient age to understand what an investigation is, and the potential consequences of providing or not providing the information being requested? You need to ensure the learner understands why the information is being collected and what you will do with it.
- Will you need to interview other people as part of the investigation? If so, you will need to let the learner know this. If during the investigation you identify additional people that need to be interviewed, you should let the learner (or their parents where appropriate) know.
- Will you need to share the information provided by the learner with other parties as part of the investigation? If so, make it clear what information will be shared with whom or what purpose.
- Whether the collection of the information may create a risk to the learner's wellbeing and safety.

You will also need to ensure you appropriately inform other people you will collecting personal information from as part of the disciplinary process.

We recommend that you have disciplinary interview specific privacy statements prepared prior and have them readily available so that you can tailor them to the specific circumstances of the investigation. This means you can take the time to get them right and are not having to create them under pressure when a disciplinary situation arises.

Using third parties to collect information

If you use a third-party provider to collect information from learners (or their parents) you are still responsible for ensuring that the requirements of the Privacy Act are

met. This includes the requirement to inform learners (or their parents where appropriate) about the collection.

It should be clear to learners (and their parents where appropriate) that the third-party provider is collecting the information on your behalf. If the third-party provider will be using the information for its own purposes this secondary use must be lawful and clearly communicated to the learner (or their parents where appropriate), and they should be given the option to opt out of providing the information.

If you use a third-party provider that collects information about learners on a regular basis to support your operations (e.g. payroll, external IT services, google classrooms) you can inform learners and their parents of these services and the information they collect, use and share through your privacy policy.

If want to use a third-party provider to collect information on a one-off basis e.g. to undertake a survey, you should ensure that you provide the-third party provider with your collection-specific privacy statement that they must then use when they are collecting the information from your learners (and their parents where appropriate).

For more information on using technology to collect information, including technology used by third parties to collect a learner's personal information on your behalf, see Chapter 16: Technologies in Education.

For more general information on using third party providers and your responsibilities under the Privacy Act see: Working with third-party providers: understanding your privacy responsibilities.

Informing learners and parents in practice

There are several ways that you can inform learners (or their parents where appropriate) about how you are collecting, using and sharing their information.

These include (but are not limited to):

- your privacy policy
- privacy statements
- enrolment forms
- entry display notices.

Your privacy policy

A privacy policy documents how you manage and protect all personal information you collect, use, and share – it is a key privacy governance document.

A privacy policy is generally broader and more detailed than a privacy statement. While a privacy statement may be specific to a particular collection of information, a privacy policy covers all personal information you hold.

A privacy policy generally includes information beyond that which is required by IPP3 or IPP3A. For example, a privacy policy should include:

- the business systems you use to collect and store personal information
- more detailed information about your security measures
- what information you hold is considered confidential information
- information about how sensitive information is managed
- a cookie policy
- how privacy complaints and breaches are handled.

Having a privacy policy shows both learners and their parents that you understand your privacy obligations, and what you are doing to ensure personal information is protected appropriately. Ensuring your learners and their parents are aware of, and can readily access, your privacy policy is a good way to keep them informed and building trust and confidence in how you protect and respect personal information.

Your staff also need to be aware of and understand your privacy policy. This awareness helps to ensure personal information is collected appropriately and isn't inadvertently used or shared for unauthorised purposes. Staff who know and understand why and how their organisation collects, uses and shares personal information will be in a better position to identify poor privacy practices, and will be able to provide meaningful assurance to learners (or their parents where appropriate) that their personal information will be protected and respected.

If you update your privacy policy, it is good practice to let your learners, and their parents, and your staff know. For example, a school or ECE service can use existing newsletters or parent communication channels to let them know the privacy policy has been updated and how they can access it. If you are a service provider, you can email your clients and provide a link to your updated privacy policy.

Privacy statements

Privacy statements, sometimes referred to as privacy notices, are more often used for specific collections of personal information.

You can have both an overarching privacy policy that covers how you collect, use and share personal information more generally, and you can develop and use tailored privacy statements for specific collections of personal information.

A privacy statement is a good way to provide learners (or their parents where appropriate) with the more detailed, collection-specific information necessary for them to make an informed decision about providing you with their personal information in those specific circumstances. You can also refer to your privacy policy in your collection-specific privacy statement – this will enable learners (and their parents) see how the specific collection aligns with your organisation's general privacy practices.

Privacy statements need to be complete, accurate and up to date – people should be able to trust and rely on the information in your privacy statements when making

privacy related decisions. As with your privacy policy, if you update your privacy statements, it is good practice to let your learners, and their parents, and your staff know.

For more information about creating privacy statement see: Office of the Privacy Commissioner | Transparency.

We have created a way for organisations to make their own privacy statements. To access our online privacy statement generator, see: Office of the Privacy Commissioner | Privacy Statement Generator.

Enrolment forms

Enrolment forms are used to collect information about a learner to support the process of enrolling a learner in an ECE service, school or with a service provider. In most cases, enrolment information will be collected from a learner's parents (or guardian).

Only information necessary for the purposes of enrolling a learner should be collected through your enrolment form. What information is necessary will depend on your organisation's circumstances.

For example:

- an ECE service may require specific information to be provided to ensure it meets its licencing requirements
- a school that provides lunches may require specific information about a learner's food-related medical conditions
- a private school may require specific information to enable relevant enrolment assessments to be undertaken
- a specialist school may require specific information to determine whether the learner is eligible and what their needs are

- a school may require specific information from a learner where the Ministry of Education has directed an enrolment under the Education and Training Act 2020.

Every enrolment form should include a privacy statement informing learners (or their parents where appropriate) about why the information is being collected, what the information will be used for, and what information may be shared with other organisations. This privacy statement should be specific to the information being collected through the enrolment form.

Your enrolment form privacy statement will need to inform learners (and their parents) what information will be shared with other people (e.g. Ministry of Education, other education agencies, other government agencies, and service providers) and why. Enrolment forms are also a good opportunity to inform learners (and their parents) of your general privacy policy – you can do this by adding a link to your organisation's privacy policy in your enrolment form.

For information about collecting information using enrolment forms see Chapter 5: Collecting Information.

Schools

Schools are required to share specific information about learners with the Ministry of Education. This information is stored in a system called ENROL.

The Ministry has an ENROL Privacy Statement that you can use as part of your enrolment form documentation. The ENROL privacy statement sets out what information the Ministry collects, what it uses the information for, how it keeps the information safe and how information in ENROL can be accessed and corrected.

You can access the ENROL privacy statement here: School Enrolment Form Guidelines | Education Counts.

ECE services

ECE services are required to share specific information about learners with the Ministry of Education. This information is stored in a system called ELI. The Ministry requires all ECE services to include specific wording relating to ELI and the Ministry's collection of learner information in their privacy statements.

You can access information about ELI and the Ministry's collection of personal information here: Guide on Early Learning Information (ELI) and Privacy.pdf.

Service providers

Service providers, particularly those receiving referrals directly from a school or ECE service, will need to inform learners and their parents at the time of enrolment into the service about any information that will be shared (and why) with the learner's school or ECE service.

Entry display notices (for CCTV cameras)

If you operate CCTV cameras, entry display notices are a good way to inform learners, their parents and other visitors that CCTV cameras are operating and are being monitored.

Entry display notices should be strategically placed in prominent entry locations e.g. property and building entry points and carparks. Displaying multiple notices is a good way to ensure maximum visibility and awareness – especially if your CCTV cameras are discreet or located in areas where people would not normally expect to be under surveillance e.g. bathroom or changing room areas. If your CCTV captures audio this should also be clearly stated on your entry display notice.

Things to consider when using entry display notices for CCTV cameras include:

- The notices should be visible and clearly readable.
- They should include details of the organisation operating the system, the purpose of its use, and who to contact should a person have concerns.

- They should be appropriate in size in relation to their placement and who will be looking for it. If it needs to be seen by younger learners, it needs to be placed at a height level at which they can see and read it.

Your organisation's privacy policy should include the use of CCTV cameras and provide more detailed information on why your organisation uses CCTV cameras including how it uses the camera footage, who it might be shared with and how you keep the footage safe.

If you use a service provider to manage and monitor your CCTV cameras and footage, you should include this in your privacy policy.

For more general information about the use of CCTV see:

- CCTV guidance.
- Responding to access requests for CCTV footage.
- CCTV and school bathrooms..

Health and learning support information

Education providers often collect health information about a learner to help support the learner through their education journey.

Health information

Information about a learner's health or medical conditions can, depending on the context, be sensitive information so extra care is required when collecting, storing, using or sharing a learner's health information.

Health information is defined in section 4(1) of the Health Information Privacy Code 2020. It is a broad definition, but in an education sector context includes:

- information about a learner's health, including medical history, including mental and physical health
- information about any disabilities and the supports a learner may require (e.g. assistance in an evacuation, reading or writing assistance for assessments or exams)
- information about any health or disability support services that are or have been provided to a learner (e.g. learning support, counselling in schools)
- any information collected before, after or in the course of and incidental to, the provision of any health or disability support service to a learner.

Purposes for collecting health information in the education sector can include:

- ensuring a school or ECE service has appropriate resources to support a learner while attending school or an ECE service

- ensuring learners with health or disabilities are able to safely participate in activities, including education out of the classroom (e.g. school camps, ECE service adventure walks)
- ensuring schools and ECE services that provide meals meet food safety standards
- providing health and disability support services including counselling
- enabling the year 7 and 8 school-based immunisation programme
- to support a disciplinary process e.g. evidence of medical or health conditions, requirement to undergo drug counselling or testing as part of a suspension condition.

Health information will in most cases also be confidential information and may be subject to professional codes of practice (for example, health information collected by a speech language therapist or a counsellor). For more information about confidentiality and professional codes of practice see Chapter 4: Privacy and Confidentiality.

For more general health information guidance and links to free health information training modules, see: Office of the Privacy Commissioner | Health.

Health agencies and the Health Information Privacy Code 2020

The Health Information Privacy Code (the HIPC) applies to all **health information** collected and held by **health agencies**.

The HIPC mirrors, to a large degree, the Information Privacy Principles (IPPs) in the Privacy Act 2020 and regulates how health agencies collect, hold, use and disclose health information.

Health agencies are defined in the HIPC as agencies, or parts of agencies, that provide personal or public health or disability support services and include:

- general practitioners, doctors, nurses and dentists

- healthcare providers
- mental health providers
- disability support service providers
- occupational health providers.

Service providers who provide health or disability support services to learners (either in the school or ECE service environment or externally) will generally be a health agency, and the HIPC will apply to health information they collect, hold, use or share.

For more detailed information on the Health Information Privacy Code see: Office of the Privacy Commissioner | Health Information Privacy Code 2020.

Schools and ECE services

Schools and ECE services may also collect and hold health information about learners.

However, just because you collect and hold health information does not mean that the HIPC applies – the HIPC only applies to health agencies.

When is a school considered a health agency?

In some specific cases, a school may be considered a health agency. This includes situations where a school provides health and disability support services to learners. For example:

- where a school operates a health or medical clinic
- where a school employs or contracts health practitioners such as a school nurse, guidance counsellors, speech language therapists or occupational therapists
- health schools and specialist residential schools.

Where your school is considered a health agency, the HIPC will govern all health information collected as part of the delivery of those health and disability support

services. The HIPC will also apply to any requests for health information collected by health and disability support services function of your school about a learner. The HIPC doesn't apply to other information collected by your school outside of the delivery of health and disability support services – the IPPs will apply to those other activities.

Other health information collected by schools and ECE services

Where a school (or ECE service) is not providing any health and disability support services themselves, they are not considered a health agency and the IPPs will apply to the collection, use and disclosure of health information about learners.

The Privacy Act will also apply to any requests for health information that you may hold about a learner.

For more information about managing a learner's health information under the Privacy Act 2020 follow the guidance in:

- Chapter 5: Collecting information
- Chapter 6: Using information
- Chapter 7: Sharing information
- Chapter 11: Keeping information safe
- Chapter 13: Managing requests for information

Health information in practice

This section provides some examples of health agencies and managing health information in the education sector.

Example - Health NZ mobile oral health services

A primary school has a mobile oral health clinic visit the school once a year. The clinic is operated by Health NZ. During the days the mobile clinic is on school

grounds, learners can visit the dentist and receive oral health checks. The school principal obtains consent from learners (or their parents) to attend the clinic and receive an oral health check.

Is the school a health agency?

No. While the mobile clinic is on school grounds, the school is not providing the oral health services – the services are provided by Health NZ. Any health information the school collects as part of facilitating the visit by the mobile oral health clinic would be governed by the IPPs.

Example - Counselling in schools

An intermediate school employs a counsellor to provide counselling services to its learners. Learners can access the counselling service through self-referrals, or referrals made by teachers or the learners family.

Is the school a health agency?

Yes, but only with respect to the information collected as part of the delivery of counselling services. All information collected as part of the delivery of the counselling services will be health information and governed by the HIPC. Any health information collected by the school outside of the counselling services will be governed by the IPPs.

Example – School based health clinic

A secondary school operates a health clinic on the school grounds. The health clinic has two nurses who provide health services to learners. Where required, the nurses will arrange referrals to external healthcare providers.

Is the school a health agency?

Yes, but only with respect to the information collected by the health clinic. All information collected as part of the delivery of health services by the health clinic will be health information and governed by the HIPC. Any health information collected by the school outside of the health clinic services will be governed by the IPPs.

Example - Holding a learner's medications

A school holds medications that specific learners require while they are attending school. The medications are held securely in the school office. A school administrator makes the medications available to the learners according to agreed protocol between the school, the learner and their parents.

Is the school a health agency?

No. The school is not providing health or disability support services. They are simply ensuring that medications learners may require while they are attending school are stored securely and are made available to the learner when they require them.

Example - Holding a learners immunisation record

Primary schools and ECE services are required to maintain immunisation registers for all learners (Health (Immunisation) Regulations 1995). The immunisation registers hold the learner's immunisation certificate.

Is the primary school or ECE service a health agency?

No. The primary school or ECE service is not delivering a health or disability support service. The requirement to maintain an immunisation register which holds the learner's immunisation certificate does not make the primary school or ECE service a health agency.

For more information about the requirement to maintain immunisation registers see: Health (Immunisation) Regulations 1995 (SR 1995/304) (as at 01 July 2022) – New Zealand Legislation.

Example - Request for health information by representative

A school administrator has received a request from a parent for all health information the school holds about their child. The learner is in year 10 and has been receiving speech language therapy from a speech language therapist employed by the school. The health information includes the sessions notes of the therapist and assessment and evaluation documentation.

Can the school administrator provide access to the health information?

In this case, as the school provides health and disability support services, it will be considered a health agency and the HIPC will apply to all personal information collected as part of the delivery of those services.

Parents or guardians of a child under 16 are their child's representatives under the HIPC. Under section 22F of the Health Act, as representatives they have a limited right to access health information about their child. A request from a learner's parent or guardian for health information is treated as a HIPC rule 6 access request.

In this case, because the learner is under the age of 16, the parent making the request is considered a representative for the purposes of accessing their child's health information.

The school administrator still needs to consider whether any refusal grounds set out in in sections 49 to 56 of the Privacy Act apply before they release the learner's health information to the parent.

The school may also hold health information collected outside of the health clinic, for example, school camp health information and information about medical or health

conditions. This health information should be considered IPP6 and the rules set out in sections 39 to 57 of the Privacy Act.

Example - Request for health information by parent (refusal)

A school operates a health clinic which is run by a school nurse who provides health services to the learners attending that school. A learner's parents make a request to the school principal for all health information about their child. The learner is in year 13 (16 years old) and has received health services from the school nurse.

Can the school principal provide access to the health information?

As the school operates a health clinic the school will be considered a health agency with respect to the health clinic. Therefore, all information collected by the school nurse in the course of providing health services will be governed by the HIPC.

As the learner is 16 years old, the parent is not automatically considered a representative. The school principal will need to assess whether the parent is acting as the learner's representative when making the request (see: Office of the Privacy Commissioner | Responding to requests for a child or young person's personal information). If the principal determines that the parent is not acting at the learner's representative, they can refuse the request.

Where the parent has been determined to be acting as the learner's representative, the request for information held by the health clinic should be considered under rule 6 of the HIPC. The principal will need to consider whether any of the refusal grounds set out in sections 49 to 56 of the Privacy Act apply before they release the learner's health information to the parent.

The school may also hold health information collected outside of the health clinic, for example, school camp health information and information about medical or health conditions. This health information should be considered under IPP 6 and the rules set out rules set out in sections 39 to 57 of the Privacy Act.

Example - ECE service providing meals

An ECE service provides meals for its learners. To ensure they are meeting food safety standards the ECE service manager requests parents provide information about any food allergies or dietary requirements their child may have. This information is used to ensure appropriate food is provided to its learners.

The allergy and diet information are health information. The ECE service is not a health agency, so the IPPs apply to the information. The ECE service manager records this information in a learner food safety register and securely stores the register in the ECE services business system. Only staff with responsibility for making or serving food within the ECE service have access to the register. Parents are asked to update food safety information every six months. When the learner leaves the ECE service the ECE service manager removes the learner's information from the current version of the food safety register.

Example - School camp health information

A school runs a year 12 camp each year. As part of the camp consent process, parents are required to review and update the health profile form for their child. The form includes all health information the school holds about the learner, and parents are asked to provide any new health information, including medication requirements.

The information collected helps the school camp managers to manage the learner's health and medical conditions while at camp.

Does the HIPC apply to the health and medical information?

No. The school is not providing health or disability support services (i.e. is not a health agency), so the Privacy Act applies to the information.

What if the school was a health agency?

If the school did provide health and disability support services, and was considered a health agency, the collection of the school camp health information would not fall under the HIPC as the school camp health information was not collected as part of the school's health and disability support services function.

Learning support information

As an education provider, you will likely collect information about learners to enable you to identify and deliver effective learning support interventions for learners with additional needs.

Learning support information will often include health and disability support information about the learner, and at times this information could be sensitive, so extra care is required when collecting, holding, using and sharing learning support information.

Learning support information, including health and disability support information, collected by a school or ECE service will generally be subject to the Privacy Act. In some cases, the learning support information may be collected by a health agency (e.g. a service provider providing health and disability support services). In this case, the health information collected by that service provider will be governed by the Health Information Privacy Code.

To ensure you are collecting, using, storing and sharing learning support information appropriately follow the guidance in:

- Chapter 5: Collecting information
- Chapter 6: Using information
- Chapter 7: Sharing information
- Chapter 11: Keeping information safe
- Chapter 13: Managing requests for information

In some cases, learning support information may be collected and held by a health agency (e.g. a service provider providing health and disability support services). In this case, the health information collected by that service provider will be governed by the Health Information Privacy Code (see Health Agencies and the Health Information Privacy Code section above).

Learning support registers

Learning support registers can help you understand and effectively respond to the needs of your learners. A register can be a tool for a school or ECE service to record information about learners that are receiving a learning support intervention, including what those interventions are and who is providing them.

Registers can be at different levels – a learner level, and a school or ECE service level.

A learner level register will contain personal information specific to the learner and their learning support needs. A school or ECE service level register can be used to provide non-identifiable information about the number of learners and the types of need and be used for resource planning and capability.

Registers, particularly learner level registers, can create privacy risk. It is important that you set up and manage your registers appropriately. Some things to think about when developing your register include:

- What is the purpose of the register? Can you achieve that purpose without a register?
- What is the minimum amount of information required for the register to be effective and achieve its purpose?
- Are you collecting new information about the learner?

- Should you get consent from the learner (or their parent) to be included on the register and what do you need to tell them about the register and the information that it holds?
- Who requires access to the register, or information contained in the register, and why?
- How will you keep the information safe? Where will you store the register?
- How will you keep the information up to date? How will you manage learners that no longer require learning support interventions?

Example - Creating a learning support register

A school principal has a number of learners with various learning support needs. The principal wants to create a register to ensure the school respond to and manage its learners needs effectively. The register also helps the principal manage resourcing and funding of learning support interventions.

The principal wants to ensure that only the minimum personal information required is collected and held in the register to protect the privacy of the learners (IPP1). As part of this thinking the principal determines:

- that the date of birth of the learner isn't necessary as the register records the year level of the learner
- the NSN is included in the register to ensure the learning support information is linked to the correct learner
- the type of need and a description of the need is important to identifying appropriate supports
- the organisation or person providing the intervention is required so the principal knows who is coming into the school to provide services and to which learners

- the date the service started helps the principal determine the effectiveness of the intervention when linked with other information like attendance and achievement information
- knowing whether the intervention is funded, and by whom, helps the principal manage resourcing
- only learners actively receiving learning support services should be visible in the register.

Having completed the upfront thinking, the principal creates the following learning support register:

A	B	C	D	E	F	G	H	I	J
First Name	**Last Name**	**NSN**	**Year Level**	**Ethnicity**	**Learning Support Need**	**Learning Support Need Description**	**Service Provider**	**Service Start Date**	**Funding**
John	Smith	xxx--xxx-xxx	10	NZ Eurpoean	Neuro Diverse Need	Epilepsy	xyz Services	xx-xx-xxxx	ORS
					Neuro Diverse Need				
					Medical Need				
					Health Need				
					Behavioural Need				
					Other				

Having created the register, the principal thinks about the other requirements of the Privacy Act. The information in the register is sensitive information, so the principal saves the register in a secure location in the school's education or learner management system (IPP5).

To further mitigate against unauthorised access, use or sharing of the information, the principal also password protects the spreadsheet, and only provides the password to staff who are responsible for managing learning support within the school (IPP5). The password is updated on a regular basis. The list of staff that have the password should be reviewed regularly to ensure it is up to date.

If the school has an education management system that enables the setting of access controls, the principal can use that functionality to ensure that only authorised staff have access to the location where the register is electronically stored. The list of staff that have access to the register should be reviewed regularly to ensure it is up to date.

The principal then creates a Learning Support Register Policy which clearly sets out why the information is being collected, what it is used for and who the information may be shared with (IPP10 and 11). Staff are made aware of the Policy and training is provided at a staff meeting.

The principal makes the Policy available to all learners (and their parents), so they are aware of the collection, use and sharing of their child's learning support information (IPP3 and 3A) and retention requirements under IPP9 and the Public Records Act 2005. The Policy also sets out how learners (or their parents) can request access to, and correction of, information contained in the register (IPP6 and 7).

Accuracy of information

It is important that you take the time to ensure any learner information that you want to use or share with others is accurate, up to date, complete, relevant and not misleading.

Maintaining accurate, up to date and complete learner information is important – it helps gives you and your governance function assurance that you can rely on the information to make good decisions and gives learners (and their parents) confidence that your decisions are robust, fair and proportionate.

Relevant information privacy principles

The Privacy Act 2020 sets out rules about ensuring personal information about learners is accurate before you use or share it. The relevant information privacy principles (IPPs) are:

Principle 8: Accuracy of personal information to be checked before use or disclosure

An education provider that holds personal information must not use or disclose that information without taking steps that are reasonable, in the circumstances, to ensure that the information is accurate, up to date, complete, relevant and not misleading.

Principle 6: Access to personal information (IPP6(2))

If a learner is given access to their personal information, they must be advised that they may request correction of that information.

Principle 7: Correction of personal information (IPP7(2))

An education provider that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure

that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

What does taking reasonable steps mean?

The Privacy Act requires you to take reasonable steps that are reasonable the circumstances, to ensure personal information about a learner is accurate, up to date, complete, relevant and not misleading before you use or share it.

What steps you may need to take will depend on the circumstances. For example, when you are making a decision that could negatively impact a learner you should take extra care to ensure the information used or shared to inform that decision is accurate, up to date, complete, relevant and not misleading.

Some reasonable steps to take before using or sharing a learners information include (but are not limited to) checking:

The source of the information

From whom and how did you receive the information? Is the information more rumour and speculation than factual in nature? You may need to verify both the source and the veracity of the content of the information received before you use or share it.

The age and status of the information

How long ago did you receive the information? You may need to check with the learner (or their parents where appropriate) that the information is still correct and up to date.

If the information is contained in a report, do you have the latest version of the report? You may need to check that you have the most up to date information, or whether the information contained in the report is still valid.

Is the information relevant to the purpose you want to use or share the information?

Is the information necessary for the purpose for which you want to use or share the information? If information about a learner is contained in a report, do you need to share the full report, or is only some of the information in the report relevant?

Is there other information about the learner that you don't hold?

Is the information you hold only part of picture? You may need to seek further information to ensure you have a complete understanding of the learner's circumstance before you use or share it others. You may also need to ensure the recipient is aware you only hold part of the information and that additional information about the learner may be required from other parties to form a complete picture of the learner and their circumstances.

Could you or others misinterpret the information without additional context?

Could the information when considered on its own be misleading? Is additional contextual information required before using or sharing the information?

Does the information contain terms that have specific meanings? You may need to ensure when sharing a learner's information any terms used are fully understood by the recipient e.g. when sharing absence information ensure the recipient is aware of the difference between justified and unjustified absence.

Is the learner (or their parents where appropriate) aware of their access and correction rights (IPP6 and IPP7)?

Does the learner know you are using or sharing their personal information, and are they aware that they can request correction of that information if they believe it is wrong? This gives the learner (or their parents where appropriate) the opportunity to request correction to their information before it is used to make a decision that may impact them or shared with others.

Why it is important to use or share accurate, up to date, complete, relevant and not misleading personal information

When you use or share out of date, inaccurate, irrelevant or incomplete information to make decisions that impact a learner, the consequences for the learner and their family can be significant.

For example:

- Information about a learner's disrupted home life was not considered when making a disciplinary decision leading to an unfair or disproportionate disciplinary outcome.
- Information about a learner's disruptive behaviour several years ago was relied on to decide about unsuitability or eligibility for a scholarship or award.
- Out of date parental contact information was used to send absence notifications resulting in the notifications being sent to the wrong address.
- The mental health of a learner who has transitioned from a male to female gender can be impacted by knowing the school or ECE services student management system records their gender as male. The learner can also be impacted when the inaccurate gender information is used or shared in reports or other documents.
- Relying on out of date or inaccurate health or medical information may impact a learner's ability to access appropriate learning support interventions or funding.
- Using anecdotal information about a learner's residential address without verifying it could impact enrolment decisions.
- incomplete, out of date or irrelevant information could negatively impact a decision on a directed enrolment.
- Sharing incorrect achievement information about a learner could result in them repeating unnecessary work.

Establishing good information management practices

Good information management practices can also help you maintain the accuracy of the learner information you hold. Some of these include:

Know where you learner information is stored

Knowing what business systems hold the authoritative learner data helps ensure you are using or sharing accurate and up to date learner information. For schools this will likely be ENROL and your student management system, for ECE services this will likely be ELI and your student management system.

Establish good collection practices

Establish collection practices that ensure only accurate and up to date information is collected from learners (or their parents where appropriate) and other people. Robust collection practices help avoid duplication, inconsistency and help maintain the accuracy of the learner information you hold.

Attach dates to learner information

When adding information to a learner's file or record, ensure you note the date the information was added to the file. This helps you to determine whether the information may be out of date or irrelevant when you are considering using or sharing it later.

Undertake data and information quality checks

Implement information quality checks (manual or automated) to identify and correct inaccurate, out of date, incomplete, irrelevant or misleading information. Data quality checks provide assurance to your governance function, and your learners and parents, that information you hold is reliable and trustworthy.

Check-in with learners (or their parents where appropriate)

Annually, or at other appropriate intervals, check in with learners (and their parents) and ask them to update any relevant learner information (for example, contact information, medical or health information, family circumstance information).

Retention and disposal practices

Regularly review information held in your learner and education management systems and assess against your data retention and disposal schedule.

Oranga Tamariki Act 1989 and Family Violence Act 2018

When using or sharing learner information under section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act, you are still required to comply with the Privacy Act IPP8 requirement to take reasonable steps to ensure you are sharing accurate, up to date, complete, relevant and not misleading information.

When a learner's wellbeing or safety is at risk there is often urgency to information requests. Where an urgent request for information about a learner is received, ensuring accuracy of the information provided is always more important than speed of response. Inaccurate, out of date, incomplete, irrelevant or misleading information can lead to decisions that may create further risk or harm to the learner.

In these situations, use or share what you know to be accurate and up to date as soon as you can, and let the requester know you will come back to them with further information once you have checked it is accurate and up to date. Also consider whether contextual information is necessary to ensure the information is complete and not misleading – don't assume that the requestor will know or understand the context of the information.

For more information about using and sharing learner information using the Oranga Tamariki Act or the Family Violence Act see Chapter 6: Using Information and Chapter 7: Sharing Information.

Keeping information safe and secure

When you collect, hold or use a learner's personal information you must keep it safe and secure.

Keeping information safe and secure helps you build trust and confidence in the way you manage your learner's personal information and protects your learner's privacy, wellbeing and safety.

Keeping learner information safe and secure isn't a 'one and done' or 'one size fits all' thing. What might be a reasonable security safeguard for some information, may not be a reasonable safeguard for other information (e.g. health information may require additional safeguards due to its sensitivity). As technology evolves, so too must your security safeguards. Keeping learner information safe and secure should always be viewed through the lens of continuous monitoring and improvement.

Relevant information privacy principles

The Privacy Act 2020 sets rules about what an education provider must do to keep learners' personal information safe and secure.

The relevant information privacy principle (IPP) is:

Principle 5: Storage and security of personal information

When holding personal information an education provider must ensure that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against:

- loss
- unauthorised access, use, modification or disclosure
- other misuse.

If you are providing information to another person so they can provide a service to your organisation, you must do everything you reasonably can to prevent unauthorised use or disclosure of that information.

What are reasonable security safeguards?

To meet the requirements of IPP5 you need to make sure you have reasonable security safeguards in place to protect your learners' personal information. Whether a security safeguard is reasonable will depend on the circumstances, but it should be practicable and actually protect your learners' data.

To help identify and implement appropriate security safeguards it helps to know:

- what learner information you hold and where it is stored
- what learner information is considered more sensitive in nature
- who needs to access learner information and for what purposes.

When deciding whether a safeguard is reasonable in the circumstances ask yourself: Could someone who shouldn't know this information see it, access it or hear it?

If the answer is yes, then the safeguards you have in place to protect the information may not be sufficient to keep the learner's information safe and secure.

Who is responsible for keeping learner information safe and secure?

Keeping information safe and secure is everyone's responsibility:

The governance function (e.g. school boards and ECE service owners) is responsible for making sure the appropriate information security policies and processes are in place to keep learner information safe and secure. The governance function is also responsible for making sure those policies are reviewed regularly and that staff receive appropriate training.

School principals and ECE service managers are responsible for making sure information security policies and processes are implemented and followed by staff, contractors, visitors and learners. School principals and ECE service managers will also be responsible for managing any information security breaches or complaints that may arise.

Staff are responsible for following information security policies and processes to make sure they are keeping learner's personal information safe and secure, including reporting any information security and privacy near misses or breaches.

Develop and implement an information security policy

A good starting point for keeping learner information safe and secure is to develop and then implement an information security policy.

Just having an information security policy isn't enough to keep your learner's personal information safe. You need to implement the safeguards set out in your policy and then test that they are working. On-going monitoring of your safeguards makes sure they remain effective.

An information security policy is a set of guidelines and rules that set out how learner information will be kept safe and secure. An information security policy should cover all formats of personal information (e.g. paper records and digital records including images, videos and audio recordings) and apply to all staff, learners, contractors and visitors. It should also include the business processes you have in place to make sure the security safeguards set out in your policy are being followed and are effective.

At a minimum, your information security policy should cover:

- purpose and scope
- roles and responsibilities
- security safeguards for:

  - digital technologies
  - paper records
  - accessing, using and sharing learner information
  - use of devices
  - retention and disposal
  - security incident and breach response
  - visitor processes

- review date and process.

Your information security policy should be accessible to all staff, learners (and their parents), contractors and visitors. This ensures everyone who works with learners' information knows what they are required to do to keep the information safe and secure.

For learners and their parents this transparency demonstrates that you have considered and implemented appropriate security safeguards to protect their child's personal information.

Security safeguards for digital technologies

As an education provider you may use a number of digital technologies that collect, use, hold and store learner information (e.g. learning platforms, apps and online tools student management systems, case management systems, finance systems and parent communication tools).

Your information security policy should document how those digital technologies will be managed to make sure learner information is kept safe and secure.

Security safeguards to protect digital technologies include:

Use privacy protective digital technologies

- Use Ministry of Education approved vendors and cloud providers where you can.

- Only use digital technologies that have been approved as privacy protective in accordance with your Digital Technologies policy (provide a link to the policy).
- Prohibit use of personal accounts for work purposes (e.g. email addresses, social media and online accounts).

Access and authentication

- Use role-based access to ensure staff only have access to learner information they need to do their job.
- Implement and use two factor authentication.
- User accounts are removed when a staff member leaves or changes role.

System security

- Keep software updated and apply security patches promptly.
- Use vendor supported systems only – avoid outdated/unsupported software.
- Use encryption.
- Restrict access to server room or network cabinet.
- Secure printing functionality should be enabled.

Data protection

- Complete daily backups of learner information and test to ensure back up process is working.
- Segregate sensitive learner information (e.g. keep finance information separate from health information).
- Use secure/encrypted channels to share learner information.

Monitoring and review

- Enable audit logs for business systems to track use and changes.
- Review audit logs for unusual access and activity (e.g. out of hours logins, repeated failed login attempts, unusual modifications to learner records, employee browsing).
- Set up alerts for suspicious activity (if available).

For more information about internet security solutions and safeguards see:

Network 4 Learning (N4L): Safety & Security Solutions | Network for Learning | N4L.

Ministry of Education: Digital Technology.

Security safeguards for digital records

Your information security policy should document how digital records will be managed to make sure information is kept safe and secure.

Security safeguards for digital records include:

- Only use approved systems, tools and apps (e.g. Student Management Systems, Google Classroom, parent communication apps, case management systems, secure email) – don't use personal devices to collect, use, store or share learner information.
- Use your own login credentials to access systems, tools and apps.
- Use strong, unique passwords or passphrases and change them when prompted.
- Use two factor authentication where available.
- Only access information held in systems, tools or apps that you need to do your role.
- Lock or log out of devices when not in use.
- Records should not be printed unless absolutely necessary.
- Report any potential or actual loss or unauthorised access, use, modification or disclosure.

For additional information on keeping digital records safe see: Chapter 16: Digital technologies.

Security safeguards for paper records

While digital technology has changed the way personal information is collected, used, shared and stored, personal information may still be held in paper form (e.g.

consent forms, handwritten learner work and assessments, meeting minutes or notes recorded in notebooks).

Your information security policy should document how paper records, will be managed to make sure information is kept safe and secure.

Security safeguards for paper records include:

- A clear desk requirement – don't leave paper records lying around when not in use.
- Don't take paper records out of the work environment.
- store paper-based information in secure cabinets.
- If possible, transfer paper-based information to an electronic form as soon as possible.
- If possible, dispose of old paper-based information using secure document destruction bins or shredders.
- Report any suspected or actual loss or unauthorised access, use, modification or disclosure of paper records.

For more information on keeping paper records safe see: Chapter 16: Digital technologies.

For more information on retention and disposal of information see Chapter 12: Retention and disposal of information.

Security safeguards for accessing, using or sharing a learner's information

Your information security policy should include appropriate security safeguards to make sure a learner's personal information is:

- only accessible to those that need it to do their job

- only used for the purposes for which it was collected (unless an IPP 10 exception applies, or section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act applies)
- only shared where there is a legal authority to do so (e.g. an IPP 11 exception applies, or section 66C of the Oranga Tamariki Act or section 20 of the Family Violence Act applies).

Security safeguards to protect against unauthorised access, use and sharing of a learner's personal information include:

- implementing access controls for systems – having appropriate access controls in place helps make sure that only those that require access to a learner's personal information can access it
- requiring use of approved digital technologies to share learner information – using approved systems or digital technologies helps make sure sharing of learner information is done in privacy protective ways
- training and awareness – training raises awareness and make sure everyone knows what information they can access, what they can use it for and who they can share it with.

For more information about using learner information see: Chapter 6: Using information.

For more information about sharing learner information see: Chapter 7: Sharing information.

Security safeguards for using devices

Your information security policy should include appropriate security safeguards to make sure devices are used responsibly.

Security safeguards for device use include:

- Devices (e.g. laptops, tablets, cell phones, cameras) must be kept secure when not in use.
- Personal devices (including cell phones, laptops, tablets, cameras or recording devices) are not to be used to collect, use, store or share a learner's personal information.
- Photos or videos must be uploaded to the secure learning management platform as soon as possible and then securely deleted from the device.

If you have a digital technology and/or an acceptable use policy, you should make sure they are consistent with your information security policy (it is a good idea to link to these related policies in your information security policy).

For more information on digital technologies, including acceptable use policies, see Chapter 16: Digital technologies.

Security safeguards for retention and disposal

Your information security policy should include security safeguards to help ensure learner information isn't held for longer than is necessary, and that information is disposed of securely.

Security safeguards include:

- All paper records must be disposed of using a secure shredder or secure document destruction bin.
- All digital records must be deleted using approved secure deletion tools or e-waste disposal services.
- All devices that hold learner information that are no longer required for use must be securely wiped of all learner information before disposal using approved e-waste providers.

For more information on retention and disposal see Chapter 12: Retaining and disposing of informationn.

Security incident and breach response

Your information security policy should include processes that make sure security incidents and breaches are reported and managed in a timely manner.

Security safeguards include:

- a requirement that all security incidents and breaches are reported
- an explanation of processes to follow when a security incident or breach (suspected or actual breach) occurs
- a requirement that all security incidents and breaches are recorded in a security incident register
- where a security incident or breach involves a learner's personal information, a requirement that the processes set out in your privacy breach management policy are to be followed (it could be helpful to explain the difference between a security breach and a privacy breach and include a link to your privacy breach management policy).

Security breach vs privacy breach

The following flowchart can help you determine when a security incident is also a privacy incident or breach of a learner's personal information.

Flowchart: Security breach vs privacy breach

Security breach vs privacy breach

Step 1: A security incident occurs

Something has gone wrong with one of your information security safeguards, for example:

- a lost laptop
- an unlocked cabinet
- a printed health report was left in the staffroom
- an email was sent to the wrong person
- an aunauthorised third party has accessed your business system.

Step 2: Was a learner's personal information involved?

No

It's a **security breach only**. Manage the security breach following the processes set out in your information security policy.

Yes

Step 3: Was the learner's personal information lost, accessed, used, altered, or shared?

Yes

Yes - it is a **security breach and a privacy breach**. Manage the privacy breach following the processes set out in your privacy incident management policy.

No

No - it's a **security breach and a near miss privacy incident**. Manage the near miss privacy incident following the processes set out in your privacy incident management policy.

Unsure

Unsure - it's a **security breach and a potential privacy incident**. Manage the potential privacy incident following the processes set out in your privacy incident management policy.

Privacy Commissioner
Te Mana Mātāpono Matatapu

For more information on privacy breach management see Chapter 15: Privacy incidents.

Visitor Processes

Robust visitor processes are essential as they help protect the safety of your learners and their information.

Visitors, whether parents, contractors or representatives from external agencies, may unintentionally or deliberately access areas or see and hear information about learners that they shouldn't.

Security safeguards for visitors include:

- All visitors must sign in at the office.
- All visitors must be issued a visitor pass that is worn at all times while on site.
- Escort visitors if they need to enter a classroom, office or staff only area.
- Challenge anyone without a visitor pass and direct them to the office to complete the sign-in process.
- Check visitors out when they leave site.

Requiring visitor sign-in processes, visible identification, and restricted access while on site helps you know who is on site and where they are and reduces the risk of unauthorised access to your learner's information.

Keeping learner information safe and secure in practice

This section provides some common examples of keeping information safe and secure in the education sector.

Example - Parent communication platforms

Education providers use parent communication platforms to share progress and achievement information and updates about learners (e.g. photos and videos of classroom activities). Teachers upload learning activity notes, photos and videos regularly, and parents log in to view their child's progress.

What are some of the security safeguards education providers should have in place to make sure learner information shared in parent communication platforms is kept safe and secure?

Consent management

- Make sure you obtain consent to take photos and videos of your learners for the purpose of posting to the parent communication platform.
- Review and update consent regularly and update the platform to reflect any changes.

Platform security

- Only use approved, secure parent communication platforms.
- Turn on and require use of multi-factor authentication where it is available.
- Use strong, unique passwords and log-in using your unique credentials(do not share log-in credentials or passwords).
- Always log out when you have finished uploading content.

Device use

- Only use approved devices for recording and uploading content - do not use personal devices.
- Devices should be locked when not in use.

Content controls

- Double check that updates and images are loaded to the correct learner profile before posting.

- Avoid posting unnecessary or sensitive learner information (e.g. health or family circumstance information).
- Photos or videos of groups of learners are not posted unless all parents have provided consent.

Access controls

- Remove access for staff who have left or changed roles.
- Remove access for parents whose children's have left the school or ECE service, or for safety reasons should no longer have access.

Example - Photos and videos used for learning portfolios

An ECE service teacher takes photos and videos of learners during structured learning activities. The photos and videos are used in learning portfolios to evidence learning progress and share updates with parents. Consent has been obtained from the learner's parents to take photos and videos for these purposes.

What should the teacher do to ensure the photos and videos are kept safe and secure?

To keep the photos and videos safe and secure the teacher should:

- Only use ECE service approved devices to take photos and videos of the learners (personal devices should not be used).
- Make sure photos and videos are uploaded directly to the ECE service's secure learning management system (e.g. Storypark, Educa) as soon as possible and then securely deleted from the device.
- Make sure photos and videos are uploaded to the correct learner profiles.
- Not print, display, post to public platforms (e.g. social media accounts) or share photos and videos of learners with third parties unless specific consent has been obtained from the learner's parents for those purposes.

- Make sure any printed copies of photos are securely disposed of (e.g. shredded).
- Make sure old photos and videos that are no longer needed are securely disposed of (do not disposed of old photos in the general rubbish).

For more guidance on filming and photography of children and young people see our guidance: Children and young people: Filming and photography.

Example - Protecting learner information in paper records

A school administrator maintains the schools paper records which include enrolment forms, consent forms, emergency contact information, health information and learning support assessments and reports.

What security safeguards should the school administrator have in place to keep the paper records safe and secure?

The school administrator should ensure:

- they are stored in locked filing cabinets or a secure records room
- a process is in place for approved safe to access/sign-out paper records and that they are returned/signed-in promptly
- sensitive paper records (e.g. records containing health information) are stored separately with restricted access
- when in use, paper records are not left unattended or used in areas where other people may be able to see or access the information
- when paper records need to be moved or copies shared with approved third parties they are placed in a sealed folder or envelop marked ‘confidential’ or “private’
- paper records are not taken off site unless absolutely essential and approved by the school principal

- old or duplicate paper records are securely disposed where permission to dispose of the records has been obtained (e.g. shredders or secure document destruction bins)
- a document disposal register is maintained for accountability purposes.

Example - Protecting learner information at meetings

A learning support team hold a meeting to discuss several learners who need additional support. To help identify appropriate supports, the team needs to access reports, assessments and other information about the learners.

How can the learning support team ensure that the learner's information is kept safe and secure?

The reports, assessments and other documents contain sensitive information that needs to be protected against loss and unauthorised access, use and disclosure. However, it is also important that learning support team can access and use the information to identify appropriate learning supports for the learners.

To keep the learner's' information safe and secure before, during and after the meeting, the learning support team should:

Before the meeting

- Book a private meeting room if it is an in-person or hybrid meeting.
- Only invite staff that have a legitimate need to be present.
- make sure meeting invites do not contain personal information about the learners.
- If preparatory documents are being sent to meeting participants in advance of the meeting send secure links to the documents where possible.
- In the meeting invite encourage meeting participants not to print copies of the documents.

- Where is it necessary to use paper documents, have one person (e.g. the meeting organiser) print the documents and provide them to meeting participants at the meeting.

During the meeting

- Maintain confidentiality – discussions should be restricted to the purpose(s) of the meeting and should not be overheard by unauthorised people.
- Don't use unapproved digital technology to record the meeting or create transcripts of the meeting.
- If there is a break in the meeting, make sure computers and display devices are locked and the meeting room is secured.

After the meeting

- Collect all paper copies of documents and make sure they are returned to a locked filing cabinet or securely disposed of (e.g. shredded or put in secure document destruction bins).
- Save meeting minutes in the schools secure document management system with appropriate access restrictions.
- Don't email meeting minutes to meeting participants – send them a link to the meeting minutes instead.

For guidance on sharing learner information at multi-agency meetings see Chapter 7: Sharing information.

Example - Using a third party to provide a service

A school principal wants to procure a new case management system to manage learning support information. The system will be provided and maintained by a third-party vendor.

What should the principal do to ensure the learning support information held in the case management system is kept safe and secure?

The school principal must make sure they do everything reasonably within their power to prevent unauthorised access, use and disclosure of learner information where it is necessary for that information to be given to a person in connection with the provision of a service to the school. While the third-party vendor is providing and maintaining the case management system, the school board is accountable for making sure the learner information is kept safe and secure.

The school principal should:

- Do due diligence before purchasing the case management system including assessing the third-party vendor's privacy policy and security standards comply with the Privacy Act.
- If the case management system is cloud based, confirm where the information will be stored (New Zealand or offshore), and determine whether overseas storage is appropriate for the data and information that will be held in the case management system (e.g. for Māori data or sensitive information).
- Identify whether the case management system offers security enhancing features such as role-based access, encryption, secure logins, multifactor authentication and audit functionality.
- Make sure the contract with the third-party vendor contains adequate data protection clauses and put in place service level agreements for system availability, backups and security maintenance and response times.
- Utilise role-based access controls to ensure only authorised staff can access the case management system.
- Require the use of strong, unique passwords and that staff log into the case management system using their own credentials.
- Make sure user accounts are removed promptly when staff leave or change roles.
- Conduct regular reviews of access and use of the case management system, access permissions and audit logs.

- When the contract expires or the case management system is no longer required, require the third-party vendor to provide a complete export of all information held in the case management system (in a useable format) and seek confirmation that the third-party vendor has permanently deleted all learner information from its servers.

Example - Protecting a learner's health information

A year 6 learner has a severe peanut allergy. The learner's parents have provided the school principal with a detailed allergy management plan, including medication requirements.

What should the school principal do to keep this information safe and secure?

The allergy management plan contains sensitive health information that needs to be protected against loss and unauthorised access, use and disclosure. However, it is also important that relevant staff know about the plan so that they can assist the learner appropriately if required.

To keep the learner's allergy management plan safe and secure, the school principal should:

- Store the paper version of the allergy plan in a secure filing cabinet in a restricted access area (e.g. the principal's office) or create a digital copy of the allergy plan and file it in a business system with appropriate role-based access (returning the original to the learner's parents).
- Enable access to the digital allergy plan for teachers and staff who require access to the allergy plan to help keep the learner safe.
- When relief staff are working with the learner make sure relevant information about the allergy plan is shared with them (e.g. via a verbal briefing or controlled access to the allergy plan).

- Share key information with other staff in need-to-know format without sharing or providing access to the learner's full allergy management plan (e.g. the learner has a severe peanut allergy, epi-pen and instructions for use are stored in the teacher's cupboard in the classroom).
- When the learner leaves the school ensure that the information is only retained for the statutory period and then is securely deleted (e.g. shredded or placed into a secure document destruction bin).

For more information about health and learning support information see Chapter 9: Health and learning support information.

For more information on retention and disposal of information see Chapter 12: Retaining and disposing of information.

Retaining and disposing of information

Education providers hold a lot of personal information about learners.

Holding only the information that you need (or are required to retain) and securely disposing of information you don't reduces the risk of unauthorised access, use or disclosure that may result in or contribute to a privacy breach.

It's also important that decisions you make about learners are informed by accurate and up to date information. Ensuring you dispose of information that is inaccurate or out of date helps ensure you make robust and fair decisions about your learners. For example, using out of date or incorrect information to inform a disciplinary decision can led to an unfair outcome and have long lasting impacts for both you and the learner.

Relevant information privacy principles

The Privacy Act 2020 (the Privacy Act) sets rules about how long an education provider can retain learner's personal information. The relevant information privacy principle (IPP) is:

Principle 9: don't keep personal information longer than necessary

An education provider that holds personal information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.

For state and state integrated schools, or any non-government organisation or private business providing services on behalf of a government department (e.g. the Ministry of Education) the retention and disposal requirements set out in the Public Records Act 2005 will override IPP9.

Relationship between the Privacy Act 2020 and the Public Records Act 2005

The Public Records Act 2005 applies to public offices and sets the rules around what information held by a public office must be retained, and for how long. Under the Public Records Act, schools (state and state integrated) are public offices and must comply with the rules set out in that Act.

A non-government organisation (NGO) or private business that provides services on behalf of a public office (e.g. an NGO providing learning support services to learners on behalf of a state or state integrated school or the Ministry of Education) will be required to comply with the Public Records Act with respect to the public records it holds as a result of providing those services.

NGOs or private businesses that are simply funded by a government agency but are not providing services on behalf of the government, are not required to comply with the Public Records Act in relation to the records held as a result of providing those services.

If you are an NGO or a private business providing services under a contractual arrangement and are unsure whether you are required to comply with the Public Records Act check with the contracting agency.

Information Privacy Principle (IPP) 9 of the Privacy Act 2020 requires that personal information is not kept longer than is required for the purposes for which the information can be lawfully used. For the purposes of IPP9, lawful purposes for use can be wider than the purpose for which information was originally obtained.

Any records containing personal information about a learner that don't fall under the rules set out in the Public Records Act 2005, must be retained and disposed of according to IPP9.

What does retention and disposal mean?

Retention

Retention is the systematic process of storing and managing a learner's information for a specified period of time making sure that information is accessible and secure until it is no longer required or can legally be disposed of.

Disposal

Disposal is the process by which an agency or organisation manages records longer required for its functions.

Disposal includes:

- securely destroying or deleting information
- transfer of information to Archives New Zealand (for state and state integrated schools'
- discharging information to the care of an organisation (e.g. a library, marae committee) or an individual (requires school board presiding member sign off).

For more information about the process for transferring records to Archives NZ or discharging records see: Managing school records - Ministry of Education.

State and state integrated schools

State and state integrated schools are required to comply with both the Public Records Act 2005 and the Privacy Act IPP9 requirements.

The key is knowing what Act applies when and what you are required to do under each.

When the Public Records Act applies

The Public Records Act 2005 is the primary legislation governing the retention and disposal of learner information. It applies to state and state integrated schools and covers school records.

Private schools and charter schools are not subject to the Public Records Act 2005 but must comply with the Privacy Act requirements for retention and disposal of a learner's personal information.

School records include learner records, correspondence, accounts, assessments and tests, school reports, meeting minutes and photos and videos of learners. Most of the information you created or receive as part of operating your school and delivering education to your learners will be a school record.

In practice most records held by a school will be covered by the Public Records Act. However, there are a couple of limited exceptions:

- work produced by a learner (where there is a reasonable expectation that the work will be returned to the learner)
- special collections e.g. contents of a school library
- unsolicited material received by a school but not related to its functions e.g. informational brochures.

School Records Retention and Disposal Schedule

Requirements for the retention and disposal of school records is set out in the School Records Retention and Disposal schedule (the Schedule). The Schedule includes information about how long to keep school records, why they are kept for that period, and what needs to happen to those records when they are no longer required.

For more information about managing school records, including the access to the Schedule, see: Managing school records - Ministry of Education.

When information privacy principle (IPP) 9 applies

Where personal information about a learner is not a school record or related to one of the limited exceptions, then the requirements of IPP9 will apply to the retention and disposal of that information.

When the retention period under the Public Records Act ends, the authorised disposal action can be undertaken. For any records being kept longer than the authorised retention period, the requirements of IPP9 will apply, meaning that the personal information can only be retained if you have a lawful purpose to use it.

ECE services

ECE services are generally not public offices, so they don't fall under the Public Records Act retention and disposal rules.

ECE services provided by a public office (e.g. a university or polytechnic) will likely be required to comply with the Public Records Act 2005 if they are providing the ECE service on behalf of the public office.

Instead, ECE services must comply with the following:

- Education (Early Childhood Services) Regulations 2008.
- ECE Funding Handbook requirements.
- ECE Licencing Criteria.
- Information Privacy Principle (IPP) 9 of the Privacy Act 2020.

The ECE service funding or licencing requirements apply to categories of records that cover all information, not just personal information about your learners. The categories include:

- funding and audit records (e.g. attendance, enrolment and fee/payment records)

- health and safety records (e.g. accident and incident reports and illness and medication records)
- licencing compliance records (e.g. policies, governance records and complaints).

It's important that you understand the information retention and disposal requirements set out in the regulations, licencing criteria and funding handbook.

For more information about managing ECE service records see: Record keeping requirements - Ministry of Education.

For more information about ECE licencing regulations and criteria see: Licensing and certification - Ministry of Education.

References to the Funding Handbook, Licencing Criteria, and GMA are correct at time of publication (March 2026). Please check the Ministry of Education or Education Review Office for updates.

When information privacy principle (IPP) 9 applies

Where personal information about a learner is not covered by retention requirements set out in the ECE regulations, ECE licencing criteria or funding requirements IPP9 will apply to the retention and disposal of that information.

Personal information that is not covered by the ECE service funding or licencing requirements may include:

Information Category	Examples
Learning and Development Records	• Teacher observations, assessment notes and internal progress tracking. • Draft teaching plans that include personal information about learners.
Parent Communication Records	• Learning stories, photos, videos and artwork. • Teacher observations, assessment notes and internal progress tracking. • Draft teaching plans that include personal information about learners.

Health and Wellbeing Information (additional to that covered in the ECE service funding or licencing requirements)	• Information parents may share about allergies, developmental needs or family circumstances. • Custody orders or information about family court matters.
Operational/Temporary Records	• Consent forms for trips or activities. • Internal memos or teacher notes about a child's behaviour.

Create a retention and disposal schedule

A retention and disposal schedule can help you manage your learner information. It can help make sure you are complying with your funding and licencing requirements and not retaining learner information longer than is necessary.

Your schedule should include your obligations set out in the ECE Licencing Criteria, the ECE Funding Handbook, the requirements of the Education (Early Childhood Services) Regulations 2008, and then what information is then subject to IPP9 requirements.

The following is an example of a retention and disposal template you could use to get you started.

Record type	Record description	Record purpose	Legal requirement to retain	Retention period
Learner Record	Enrolment records	Enrolment agreements are used by the Ministry of Education to verify the days/sessions that each child is	ECE Funding Handbook 6-1 ECE Licencing Requirement to collect information in enrolment forms (GMA 10)	ECE Funding Handbook 6-1 retention requirement: 7 years after child leaves the service

		enrolled for and expected to attend		
Learner Record	Attendance records	Attendance records are used by the Ministry of Education to verify that children have attended the service as claimed and to identify that absence rules have been applied correctly	ECE Funding Handbook 6-3 ECE Licencing Requirement to maintain an attendance record (GMA 11)	ECE Funding Handbook 6-3 retention requirement: 7 years after child leaves the service
Learner Record	Incident/Accident reports	All practicable steps are taken to get immediate medical assistance for a child who is seriously injured or becomes seriously ill, and to notify a parent of what has happened	ECE Licencing Requirement HS27 to have records available for inspection	IPP9 Privacy Act - securely delete records when no longer required for a lawful purpose
Learner Record	Learner stories			IPP9 Privacy Act – securely delete when no longer required for lawful purpose

Non-government organisations (NGOs) and service providers

Non-government organisations (NGOs) and private businesses are not public offices, so they don't fall under the Public Records Act retention and disposal rules. Instead, NGOs and private business must comply with IPP9 of the Privacy Act.

Providing services on behalf of a public office

Where an NGO or private business is providing services to a learner on behalf of a public office (e.g. on behalf of a state or state-integrated school or the Ministry of Education) then the records collected and held as a result of providing those services will be public records and subject to the requirements of the Public Records Act 2005.

Care records

Archives NZ has issued a temporary care records protection instruction.

The temporary protection instruction applies to care records created, received or held by public offices. Its purpose is to protect State care records while work is undertaken to review the retention and disposal of State care records.

The effect of the temporary protection instruction means that all State care records must be retained. They must not be disposed of, altered or destroyed without the permission of Archives NZ (you can still transfer care records to Archives NZ).

The temporary protection instruction also applies to records relating to work non-government organisations (NGOs) have carried out on behalf of government organisations covered by the temporary protection instruction.

For more information about Care Records see:

- Temporary care records protection instruction – Archives New Zealand

- Care records definition – Archives New Zealand

Archive NZ is currently reviewing the retention and disposal settings for care records. You should check the Archives NZ care record webpage for updates on managing care records.

Retention and disposal in practice

This section provides some common examples of retaining or disposing of information in the education sector.

The Care Records Temporary Protection Instruction must be considered when considering retention and disposal of Care Records.

This means that some information that could be disposed of under existing retention and disposal requirements may need to be retained to meet the requirements of the Care Records Temporary Protection Instruction.

Example - Learner's own work created in the classroom

During the year work created by the learners is displayed in the classroom. This work includes artwork, short stories and poems, and crafts.

In general, a learner's own work (e.g. classwork, artwork, assignments) is not considered a school record – they are created by the learner as part of their day-to-day learning. If the work identifies the learner (e.g. contains the learner's name or other identifying information) it will be considered personal information and subject to the requirements of IPP9.

When tidying up a classroom at the end of term, or end of the year, it is a good idea to ask your learners (or their parents in the case of younger learners) whether they

would like their work returned to them. If they don't want the work returned, then you can securely dispose of it.

Example - Learner assessment information

Work submitted by a learner for formal assessment (e.g. exams, internal assessments, portfolios) is considered the learner's own work. Where there is an expectation that the work will be returned to the learner, then the work submitted by the learner will not be a school record.

If the work is required to be retained as evidence of the assessment results, then the work would be considered a school record and must be retained for the period specified in the School Records – Retention and Disposal Schedule.

The results of the assessment (e.g. marking and any comments made by the marker) are school records and must be retained for the period specified in the School Records – Retention and Disposal Schedule.

Managing requests for information

As education providers you will likely spend a lot of time responding to requests for information about your learners.

Requests can be made by learners, other people (e.g. a learner's representative), or other agencies and organisations.

Knowing how to respond to different types of requests, and having good processes in place, will help you manage and respond to requests in an effective, timely and privacy protective way.

Relevant information privacy principles

The Privacy Act 2020 provides a learner (or their representative) the right to access or correct their personal information. The relevant information privacy principles (IPPs) for access and correction of personal information are:

Principle 6: Access to personal information

A learner (or their representative) is entitled to receive upon request:

- confirmation of whether you hold any personal information about them
  and
- access to their personal information.

When providing access to a learner (or their representative) you must advise them that they can ask for correction of that information.

Principle 7: Correction of personal information

A learner (or their representative) is entitled to request correction to their personal information.

When requesting correction of their information, or at any other time, the learner (or their representative) is entitled to:

- provide you with a statement of correction
  and
- request that you attach that statement to the information (if you decide not to correct their information).

You must take steps that are reasonable in the circumstances to make sure that the information you hold is accurate, up to date, complete and not misleading (having regard for the purposes for which the information may lawfully be used).

If you decide not to correct a learner's information that you hold, and you have been provided with a statement of correction, you must take steps that are reasonable in the circumstances to make sure the statement of correction is attached to the information in a way that ensures it will always be read with the other information you hold about the learner.

If you have previously disclosed the information, you must, in so far as is reasonably practicable, inform the people to whom you have disclosed the information of the correction.

Access requests (IPP6)

Every learner (or their representative) has the right to access their personal information (IPP6).

You must give reasonable assistance to any learner (or their representative) who wants to or has made a request to access their personal information. This includes helping them to make the request and working with them to clarify what information they are asking for.

The Privacy Act (sections 39 to 57) then sets out the rules you must follow when responding to an access request, including the circumstances in which you can decline the request.

Responding to an access request

There are several steps to follow when responding to an access request:

Step 1: Identify what information is being requested.

If the request is vague or too broad, contact the requester to clarify what personal information they are requesting.

Step 2: Work out whether you hold the personal information requested.

Step 3: If you don't hold the personal information, decide whether the request should be transferred to another agency.

If you decide that an access request should be transferred to another agency, you must transfer the request to the agency and tell the requester within 10 working days of receiving the request.

Step 4: Decide whether you will provide the information or refuse the request (in part or in full).

Step 5: Tell the learner (or their representative) of your decision no later than 20 working days after you received the request.

Step 6: Make the information available to the learner (or their representative) if you have decided to give them access.

Step 7: Record the details (e.g. date received, requester details) and outcome of the request (e.g. decision and date of decision, information provided to requester).

When is a requester a representative?

Under the Privacy Act, a representative is a person who is lawfully acting on the learner's behalf.

For more information about who can be a representative see our guidance: Office of the Privacy Commissioner | Responding to requests for a child or young person's personal information.

Under the Health Information Privacy Code, a parent or guardian will be a representative of a learner under the age of 16 years. For more information about health information see Chapter 9: Health and Learning Support information.

For more information about health information and the Health Information Privacy Code see our guidance: Office of the Privacy Commissioner | Health Information Privacy Code 2020 and Office of the Privacy Commissioner | Health.

What do you need to tell the learner (or their representative)?

When you tell a learner (or where appropriate their representative) of your decision in **step 3**, you must inform them of the following if:

- you do not hold the information requested

  or
- you do not hold the information requested in a way that makes it readily retrievable

  or
- you do hold the information requested, and access to all, or some, of that information has either been granted or refused

  or
- you neither confirm nor deny that you hold information about the learner to whom the request relates.

If you have **granted access** to all, or some, of the information requested, you must tell the learner (or their representative) about:

- The way the information will be made available. If the way you are making the information available is different to their preferred method, you need to tell them why.
- The charge (if any) payable, and whether all or part of that charge is payable in advance.
- The learner's (or their representative's) right to make a complaint to the Privacy Commissioner about the charge.

For more information about charging for access requests see our guidance: Charging for access to personal information.

After notifying the learner (or their representative) of the decision to give them their information, the way the information will be made available, and any charge payable, you must then give the information to the learner (or their representative) without due delay.

Ways to grant access to information

There are a several ways you can provide a learner (or their representative) access to their personal information.

If the information is contained in a document, you can:

- give the learner (or their representative) an opportunity to inspect the document
- provide the learner (or their representative) a copy of the document (digital or hardcopy)
- give the learner (or their representative) a summary of the document
- where the document is an article, or a thing from which sounds or images are capable of being reproduced, enable the learner (or their representative) to hear or view the sounds or images

- tell the learner (or their representative) verbally of the information about them in the document.

Unless there is good reason not to do so, you must make the information available to the learner (or their representative) in the way they prefer.

Responsibilities before providing access to personal information

Before you provide access to the learner's personal information you must:

- be satisfied of the identity of the requester
- not provide access if you have reasonable grounds to believe the request has been made under the threat of physical or mental harm
- ensure that information intended for the learner (or their representative) is only received by them.

For more information about confirming the identity of the requester see our blog post: Office of the Privacy Commissioner | Confirming a requester's identity.

Refusing an access request

In general, you must provide a learner (or where appropriate their representative) access to their personal information. However, there may be some circumstances where that's not appropriate.

The Privacy Act provides several refusal grounds that cover different circumstances including:

- protection of an individual
- evaluative material
- other administrative reasons

Some commonly used refusal grounds for education providers might include:

- You don't hold the information.
- Providing access to some or all of the information could negatively affect the learner's mental health.

- The learner is under the age of 16 and providing access to the information would be:
  - contrary to their interests or
  - contrary to the interests of another individual to whom the information relates and who is also under the age of 16.
- Providing access would pose a threat to the health and safety of the learner or another person(s.)
- Providing access would include sharing information about a victim of an offence and cause the victim significant distress, loss of dignity or injury to their feelings.
- Providing access would involve the unwarranted disclosure of the affairs of another person.
- Providing access would breach legal professional privilege.
- The request is frivolous or vexatious, or the information is trivial.

Deciding that a refusal ground applies to a piece of information should be a considered decision. In cases where you don't hold the information, the decision will be a simple one. In cases where you believe that granting access will cause harm to the learner or another person, the decision may be more complex.

For schools, it will usually be your privacy officer that is responding to access requests, including refusing requests. In more complex situations you should consider keeping your school board or ECE service managers informed.

If the personal information requested is contained in personal communications (e.g. emails, text, online messaging apps), this will not be a reason to refuse an access request.

What do you need to tell the learner (or their representative)?

If you have **refused access** to all, or some, of the information requested, you must tell the learner (or their representative):

- The reason for the refusal or reasons for refusal for each deletion within a document or masking in a digital image.
- The grounds on which the reason for refusal was made if you have refused the request on the basis of the information being evaluative material.
- The grounds on which the reason for refusal was made (for refusal grounds other than evaluative material) if the learner (or their representative) asks for those grounds.
- The learner's (or their representative's) right to make a complaint about the refusal to our Office.

Redacting information from documents

In some cases, personal information about a learner will be in documents or digital images that contain information about other people. A digital image includes, but is not limited to, photos, videos, CCTV recordings, audio recordings. This is often referred to as 'mixed information'.

Where you have determined that a refusal ground applies to some of the information contained in the document or digital image you can grant access to that document with appropriate deletions (also called redactions) to information that you've decided should be refused.

Remember, you are required to inform the learner (or their representative) of the refusal grounds. If you are using different refusal grounds for different sections of the document or digital image you need to tell the learner (or their representative) about the refusal ground used for each deletion.

Granting access with conditions

Where you have determined that a refusal ground applies, you can decide to grant access to the information with conditions relating to the learner's (or their representative's) use of the information and disclosure of the information to another person

Conditions could include enabling the requester to view the information on site (rather than providing a copy of the information), and restrictions on sharing the information (e.g. posting the information online, or otherwise on-sharing the information to third parties). Restrictions will be more relevant where a document contains personal information about others.

Access directions

An access direction is a binding written notice issued by the Privacy Commissioner. An access direction can be issued if the Privacy Commissioner has investigated an IPP6 complaint and the Commissioner has determined that the requester is entitled to some, or all of the information requested.

For more information about Access Directions see our page: Access Directions.

Additional guidance

For more information on access requests, including refusal grounds, charging and access directions, see:

- Our general IPP6 guidance, including information on specific refusal grounds: Office of the Privacy Commissioner | Principle 6 - Access to personal information.
- Poupou Matatapu: Responding to access and correction requests well: Office of the Privacy Commissioner | Responding to requests and complaints well.
- Access Directions: Office of the Privacy Commissioner | Access directions.

Responding to access requests in practice

The following section provides some examples of how to respond to access requests in the education sector.

Example - non-custodial parent requesting information about their child

A parent currently living overseas requests all the personal information that a school holds about their child. The child is a learner in year 4. The requester did not complete or sign the enrolment form, and the school holds no information about them. Teachers and other staff have never heard the learner talk about the overseas parent.

Can the school's privacy officer provide access to the information?

The privacy officer will first need to determine whether the requester is acting as a representative for the learner. If the Privacy Officer determines that the requester is acting as the child's representative, they will then need to:

- decide whether to provide access or not
- if they decide to grant access, consider whether any refusal grounds apply
- confirm the identity of the requester before providing access to the learner's information.

For more detailed guidance on how to determine whether a requester is acting as a representative for the child and whether the Privacy Officer can provide access to the information in this case see our guidance: Office of the Privacy Commissioner | Responding to requests for a child or young person's personal information.

An email address or contact number on their own won't necessarily provide assurance of identity, but they may form part of the evidence you collect to confirm the requester's identity.

The privacy officer should talk to the school principal about whether any of the learner's information should be shared with the non-custodial parent under section 103 of the Education and Training Act.

Example - Request from Lawyer for the Child

An Early Childhood Education (ECE) service manager receives a request from a lawyer requesting information about a learner who attends the ECE service. The lawyer advises that they have been appointed by the Family Court to represent the learner in court proceedings and provides evidence of their appointment.

Can the ECE service manager provide access to the information?

Yes, they can. A Lawyer for the Child is a specialist lawyer appointed by the Family Court to represent the interests of the child or young person in Family Court proceedings involving care of children or guardianship issues, or situations of family harm.

To fulfil their responsibilities, the Lawyer for the Child often needs information about the child or young person held by agencies such as a school or healthcare provider. When making a request for information, the Lawyer for the Child will be acting as a representative for the child or young person.

The Lawyer for the Child should always provide evidence of their appointment and brief from the Family Court. (A Lawyer for the Child is appointed by Court Minute and receives their brief by letter from the Court.) If it's not clear whether the requester is acting as the Lawyer for the Child, you should ask them to provide evidence of their appointment before providing access to a learner's personal information.

For more information about Lawyer for the Child, including guidance from the Law Society see: Is a lawyer for child the child's agent under the Privacy Act? | Office of the Privacy Commissioner.

Example - Refusal Ground –under 16, not in child's best interest

A year 9 learner disclosed personal information about their homelife to a teacher. The teacher referred the learner to the school guidance counsellor who supported the learner through that time. The issues raised by the learner did not impact the learner's educational achievement or their relationships with teachers or other learners. The learner's homelife has improved and they no longer see the guidance counsellor.

The learner's parents have made an access request as representatives of the learner. The school privacy officer has identified all the information the school holds about the learner but is concerned about providing access to the information recorded by the school guidance counsellor. The guidance counsellor noted in the learner's file that the learner did not want this information shared with their parents.

Should the privacy officer provide access to the information to the learner's parents?

If the privacy officer determines that the parents are acting as representatives of the learner, they then need to consider whether any refusal grounds apply. In this case, the privacy officer has identified information that the learner expressly stated they did not want shared with their parents.

As the learner is under 16, the privacy officer can consider the section 49(1)(c) refusal ground which states that:

"*…access to personal information may be refused where the individual concerned is under the age of 16 and the disclosure of the information would be contrary to the interests of the individual concerned*".

If the privacy officer considers refusal under this ground is appropriate, they must:

- tell the parents (in their capacity as representatives) that access to some of their child's personal information has been refused

- the specific refusal ground relied on
- that they can make a complaint about the refusal to the Office of the Privacy Commissioner.

Example - Mixed information and protecting victims

A school has commenced an investigation into a serious learner on learner assault that occurred on school grounds. The assault was committed by a year 12 learner. The learner and their parents were interviewed and had an opportunity to provide information during the investigation. At the completion of the investigation, the presiding member of the school board determined that the learner should be expelled and informed the learner and their parents in writing of the reasons for the board's decision. The parents of the expelled learner have written to the school principal requesting a copy of the full investigation report.

The investigation report contains mixed information e.g. personal information about other learners (victim and witnesses), and teachers. The victim of the assault has been significantly impacted, both mentally and physically by the assault. The victim has indicated they don't want information about how the assault affected them disclosed to other people. The learners who witnessed the assault have also been affected: some also requiring time out of school. The school principal is concerned that disclosing the personal information about the victim and other learners could cause them on-going harm and distress.

Can the school principal provide access to the full investigation report?

The school principal will first need to determine whether the learner's parents are acting as their representative. In this case, because the learner is in year 12 and is likely old enough to make the access request themselves, the learner should authorise their parents to exercise their IPP6 rights on their behalf. The school

principal could ask the parents to provide confirmation that the learner has provided that authorisation.

If the learner has provided authorisation, and there are no other factors that show it wouldn't be in the learner's best interests for their parents to exercise their IPP6 rights on their behalf, it would be reasonable for the school principal to decide the parents are acting as the learner's representative.

The school principal then needs to consider whether any refusal grounds apply to the disclosure of the investigation report in full or in part. While the investigation report contains personal information about the learner, it also contains personal information about other learners, including the victim. The school principal is aware that both the victim and other learners have been significantly impacted by the assault.

The refusal ground set out in section 53(b)(i) of the Privacy Act enables the school principal to refuse access to personal information to protect against the unwarranted disclosure of affairs of another person. This refusal ground is designed to protect the privacy of people other than the requester. To determine whether the disclosure of the victim's information is unwarranted, the school principal must balance the interests of the requester against those of other people mentioned in the investigation report.

In this case, the disclosure of certain information about the victim would likely be unwarranted for the following reasons:

- The information about the impact to the victim's mental health is sensitive in nature.
- The victim has indicated they don't want information about them to be disclosed to the perpetrator.
- Disclosure would likely cause distress to the victim.
- The perpetrator is not aware of how the assault affected the victim's mental health.

However, the principal could consider whether it is possible to provide parts of the investigation report (e.g. excluding the victim's comments about the impacts), or whether a summary of it could be provided, which would go some way to providing an understanding of the information the board considered.

For more information about the unwarranted disclosure of affairs of another person refusal ground see our guidance: Unwarranted disclosure of another person's affairs.

Example – Request for CCTV footage

A primary school received a complaint that a learner was using their cell phone during lunch breaks which was against the school's no cell phone policy. The complainant stated that a group of learners were videoing other learners in the school grounds.

The school administrator reviewed the school's CCTV footage and observed several occasions where a group of learners appeared to be using a cell phone to record other learners. From the CCTV footage, the administrator was able to identify the year 8 learner who owned the cell phone. The learner and their parents had recently been warned about previous cell phone use at the school and reminded about the no cell phone policy. A disciplinary process was commenced, and the learner's parents requested a copy of the CCTV footage.

Can the school administrator provide access to the CCTV footage?

The school administrator will first need to determine whether the learner's parents are acting as their representative. In this case, because of the age of the learner, and the fact that the parents are acting on behalf of the learner through the disciplinary process, it would be reasonable for the school administrator to decide that the parents were acting as the representative of the learner when making the request for the CCTV footage.

The school administrator then needs to consider whether any refusal grounds apply to the disclosure of the CCTV footage. While there are other learners identifiable in the footage, the administrator needs to balance the rights of the learner to be able to defend the allegations against them, and the privacy rights of the other learners seen in the footage.

The footage itself is not particularly controversial and would unlikely be an unwarranted disclosure of the affairs of other learner's (section 53(b)(i) refusal ground). In this case, it is not likely that any other refusal grounds that would apply to the CCTV footage in question.

While no refusal grounds might apply, there are some things the school administrator could consider that safeguard the privacy rights of other learners who are identifiable in the CCTV footage. If the CCTV functionality enables the administrator to blur the images of the other learners, then this functionality should be used before the footage is made shared with learner's parents. If that functionality isn't available, they could ask the learner's parents whether they would be happy to view the CCTV footage onsite rather than receiving a copy of the footage.

For more information about responding to requests for CCTV footage see our guidance: Responding to requests for CCTV footage.

Example - Refusal based on physical or mental health of the learner

A school guidance counsellor has received a request from a year 12 learner for all information the counsellor has collected about the individual during their counselling sessions over the last two years. The learner has experienced significant mental health concerns over that time, including depression. While the learner is currently in a good space with their mental health, the counsellor is concerned that disclosing the session notes which contain information from when the learner was quite unwell may negatively impact them.

Can the guidance counsellor refuse access to the information?

As a year 12, the learner is old enough to exercise their IPP6 rights and request access to their personal information. However, there are genuine concerns that disclosing the information to the learner could impact their mental health.

The counsellor could consider refusing access under section 49(1)(b) of the Privacy Act. This refusal ground can be used where the information relates to the learner, and the disclosure of the information relates to the physical or mental health of the learner and would likely impact the learner's health.

The counsellor would first need to consider whether it is practical to consult with the learner's health practitioner. If the learner has not engaged with a health practitioner in respect of these issues, then consultation may not be practical.

The counsellor should also consider whether:

- a summary of the information might be more appropriate
- they could talk to the learner about any concerns they may have
- whether they could provide access with conditions e.g. having a trusted person sit with the learner while they read the information onsite.

The right response will depend on the circumstances and the potential risk to the learner and their physical or mental health.

For more information about refusing access requests in the grounds of physical or mental health see our guidance: Prejudice physical or mental health.

Example - Request for an online assessment questions and answers

A secondary school uses a third-party provider for assessments of learners so they can identify learning support needs. A learner, with the assistance of a teacher, completes the online assessment. The assessment tool provides a report that is used to identify appropriate supports for the learner. The report provided to the school does not contain the questions asked or the learner's answers to them.

A year 11 learner has recently completed an online assessment. The assessment report was provided to the teacher and the learner and their parents. The learner's parents have contacted the school principal raising concerns about the report and asked for a copy of the assessment questions asked in the online assessment tool and the answers provided by their child. The learner has advised that they are happy for this information to be provided to their parents.

Can the school principal provide the information?

The assessment tool, including the questions that make up the assessment and the answers provided by the learner, is provided by a third-party provider. The school does not hold a copy of the questions used by the provider to complete the assessment, or the answers that the learner gave to those questions. Therefore, it is the third-party provider that holds that part of the information requested by the parents, not the school.

The assessment questions are not personal information so are outside the scope of the Privacy Act. The answers the learner provided to those questions are personal information but as the school does not hold that information this part of the request will need to be transferred to the third-party provider.

In this case, the school principal should inform the learner's parents:

- that they do not hold the information requested
- the assessment questions are not personal information about the learner so IPP 6 of the Privacy Act does not apply to that part of the request
- that they will transfer the request for the learner's answers to the assessment questions to the third-party provider (unless the parents inform the school principal that they do not want the request transferred).

Correction requests (IPP7)

Every learner (or their representative) has the right to request correction of their personal information (IPP7).

You must give reasonable assistance to any learner (or their representative) who wants to or has made a request to correct their personal information. This includes helping them to make the request and working with them to clarify what information they're wanting to correct.

If you decide not to correct a learner's personal information, they (or where appropriate their representative) can ask you to add a statement of correction to the information in dispute.

The Privacy Act (sections 58 to 65) then sets out the rules you must follow when responding to a correction request.

Responding to a correction request

There are a number of steps to follow when responding to a correction request:

Step 1: Identify what information the requester wants corrected.

If the correction request is unclear, contact the requester to clarify what personal information they want corrected, and how they want it corrected.

Step 2: Work out whether you hold the personal information that the request relates to.

Step 3: If you don't hold the personal information, decide whether the request should be transferred to another agency.

If you decide that a correction request should be transferred to another agency, you must transfer it to the agency and tell the requester within 10 working days of receiving the request.

Step 4: Decide whether you will correct the information or not.

Step 5: Tell the learner (or their representative) of your decision no later than 20 working days after you received the request.

Step 6: If the learner (or their representative) requests a statement of correction to be added to the information, decide whether you will attach the statement of correction of not.

Step 7: Tell the learner (or their representative) of your decision about the statement of correction no later than 20 working days after you received the request.

Step 8: Record the details (e.g. date received, requester details, correction requested) and outcome of the request (e.g. decision and date of decision for request and statement of correction).

What do you need to tell the learner (or their representative)?

When telling the learner (or their representative) about your decision in **step 4**, you must also tell them that:

- you have corrected, or will correct, the information. Also tell them what you have done, or will do, to correct the information

  or
- you will not correct the information and the reasons for that decision. Also tell them that the learner (or their representative) can provide a statement of correction and request that statement be added to the learner's information, and that they can make a complaint to the Privacy Commissioner.

When telling the learner (or their representative) of your decision in **step 6**, you must also tell them that:

- you have added the statement of correction to the learner's information and the actions you have taken to add the statement of correction

  or

- you haven't added the statement of correction to the learner's information, and the learner can make a complaint about the refusal to the Privacy Commissioner.

Refusing a correction request

If you consider that the learner's information you hold is accurate, you don't need to correct it.

There might be a good reason why you can't correct the information requested. For example, a learner's sex information must be recorded in your student management system as their sex registered on their birth certificate in accordance with prescribed Ministry of Education data standards (compared to a learner's gender which can be changed to record their preferred gender at any time).

However, you are required to ensure all learner information is accurate, up to date, complete, relevant and not misleading before you use or share it (IPP8). Decisions made using inaccurate information can have significant short- and long-term consequences for the learner. So, it is a good idea to carefully consider the accuracy of the information in question when you receive a correction request.

For more information about accuracy of learner information see: Chapter 8: Accuracy of Information.

Statement of correction

When you refuse a request to correct a learner's information you must advise the learner (or their representative) of their right to ask for a statement of correction to be added to the information in question.

A statement of correction should clearly set out the information the learner (or their representative) believes is wrong or incorrect and explain what the correct information should be.

When you add a learner's statement of correction, you need to make sure you're adding the statement of correction to the correct information – if you're unsure, confirm with the learner (or their representative) exactly what information they want the statement of correction added to.

You also need to attach the statement of correction in a way that ensures it will be seen and is available to be read whenever the information that has been disputed by the learner (or their representative) is accessed.

Adding a statement of correction to a digital file may be more complex that a paper file. How you add a statement of correction to a digital file will vary depending on the functionality of your systems. It may be necessary to add it into multiple places.

When adding a statement of correction to a digital system appropriately naming the statement of correction file can help ensure the statement of correction is easily accessible and clearly associated to the original document e.g. '*Statement of Correction to File [insert name of file], [insert date of Statement of Correction]*'.

Does correction include deletion?

Yes, the definition of 'correct' includes deletion. However, if you've collected that information for a specific purpose, you're allowed to keep that information for as long as it is necessary for that purpose (IPP9).

Schools and other organisations subject to the Public Records Act 2005 are required to keep certain information for specified periods. If this is the case, then you can refuse a request to delete a learner's personal information.

If you have received a correction request that asks for information to be deleted, it is best practice to record your reasons for refusing to delete the information.

Additional Guidance

For more information on correction requests see:

- Chapter 12: Retention and disposal of information
- Our general IPP7 guidance: Office of the Privacy Commissioner | Principle 7 - Correction of personal information.
- Poupou Matatapu: Responding to access and correction requests well: Office of the Privacy Commissioner | Responding to requests and complaints well.

Responding to correction requests in practice

The following section provides some examples of responding to correction requests in the education sector.

Example – Request to correct information in an investigation report about a learner's misconduct

A school principal completed an investigation into alleged misconduct of a learner. An investigation report was completed for the school board that recommended the learner be suspended for several days. The learner and their parents were provided a copy of the investigation report prior to the school board considering the report and deciding on the disciplinary outcome.

The learner's parents have made a request to the principal for certain information within the report to be corrected. In particular, the learner and their parents don't agree with the conclusions drawn about the actions of the learner from the evidence available. They've requested that certain conclusions are removed from the report.

Can the school principal refuse to make the corrections?

The school principal will first need to determine whether the learner's parents are acting as their representative. In this case, the parents have been acting as the

learner's representative throughout the investigation process so it would be reasonable to decide that the parents are acting as the learner's representative when requesting changes to the investigation report.

If the school principal decides the information in the report is correct, they can refuse the correction request. However, when they tell the learner and their parents of the decision, they must also tell them about their right to request a statement of correction be added to the report. If the learner and their parents provide a statement of correction, this should be added to the investigation report in a way the ensures the two documents will be read together.

If the school principal decides that corrections requested should be made, they should correct the investigation report. Once the amendments are made, the school principal should check with the learner and their parents that the amendments reflect the corrections they were seeking.

Example – Request to correct name and gender of learner

A school principal receives a request from a learner's parents to change their child's name, sex and gender in the school's student management system (SMS). The learner is in year 7.

Can the school principal make these changes in the SMS?

The school principal will first need to determine whether the learner's parents are acting as their representative. In this case, the learner is likely too young to exercise their right to request correction of their information. If the school principal considers that the parents are acting in their child's best interests, then it would be reasonable to determine that the parents are acting as their child's representative.

The school's SMS system enables the recording of a learner's name, sex and a variety of gender identities. The school principal can update a learner's gender in the

SMS but can't amend the sex field. The school principal is legally required to record a learner's sex as that shown on the learner's birth certificate or passport.

With regards to the learner's name, the SMS system records both legal name and preferred name. The school principal can amend the learner's preferred name, but the legal name must reflect the name on the learner's official documentation.

The school principal should inform the learner's parents of the changes that can be (or have been) made, and the reasons why some of the learner's information (legal name and sex) can't be corrected.

It's a good idea if, before making the changes, the school principal talks to the learner and their parents about any downstream impacts of updating the SMS e.g. reports that will show the learners name and gender or communications sent to parents. This enables the learner to make an informed decision about changing their name and sex information in the SMS.

Example - Request to correct an external report

A learning support coordinator has been working with a Year 13 learner and an occupational therapist to identify and provide appropriate supports to the learner. The occupational therapist completed an assessment and prepared a report. The learner is unhappy with some of the report and has made a request to the learning support coordinator for that information to be corrected.

Can the report be corrected?

In this case, the health assessment report has been completed by an independent health practitioner. This means that only the occupational therapist can make changes to their report.

The learning support coordinator should inform the privacy officer of the request so it can be transferred to the occupational therapist to consider. The learner should be

informed that the request will be transferred to the occupational therapist and the reasons why.

When a request should be managed as an Official Information Act (OIA) request

The Official Information Act 1982 (OIA) enables a learner (or their representative) to make a request for 'official information' (certain information held by public sector agencies). Official information can include personal information about other people, including other learners.

Where the person requesting the information isn't the learner (or their representative), the request should be considered under the OIA.

For more information about whether the Privacy Act or OIA apply, including a helpful table, see: Office of the Privacy Commissioner | Responding to requests for a child or young person's personal information.

Other information requests

Outside of access and correction requests, you may receive requests for information about learners from third parties.

When you receive a request for information about a learner, you shouldn't share their personal information unless you have a legal authority to do so. Legal frameworks that enable the sharing of personal information include:

- the Privacy Act (IPP11)
- the Oranga Tamariki Act (section 15, section 66 and section 66C)
- the Family Violence Act (section 20).

For more detailed information about sharing learner information see Chapter 7: Sharing information.

Managing privacy complaints

It is important to have a documented process for handling privacy complaints.

Managing privacy complaints well can prevent a small problem becoming bigger and reduce the potential of harm (or further harm) being caused to the learner affected.

Complaints can be an indicator of problematic privacy practices or be made as result of a privacy breach. A privacy complaint provides an opportunity to review your privacy policy, processes and practices and make improvements where necessary.

Have a privacy complaints process

You should have formal privacy complaints process that people can access when they have a privacy concern. This can be part of a broader complaints process or be a standalone process for privacy complaints.

An effective privacy complaints process will:

- enable quick resolution
- promote good decision making
- identify and enable timely and effective responses to privacy breaches
- build and maintain good relationships.

Your complaints process should be user friendly, and enable complainants to be heard, understood, and respected, and maintain confidentiality of any information provided. Learners (or their parent's where appropriate) should be able to make a complaint about how their personal information has been collected, used or shared if they choose to so your complaint process should enable them to do so.

At a minimum, your privacy complaint process should:

- be fit for purpose for your organisation
- be easily accessible to staff, learners, parents and the broader public e.g. published on your website, accessible through parent portals
- have clear processes for both staff and the complainants to follow
- provide different ways for making the complaint e.g. online form, email, phone number
- be clear on who will be managing the complaint process and the process for escalation
- provide timeframes for responding to complaints
- provide steps a complainant can take if they are not satisfied with the outcome.

Leaders and managers should receive regular privacy complaint and outcome reports. This information can help your leaders and managers identify privacy process and practice improvements.

For information on setting up your privacy function see Chapter 3: Privacy is everyone's responsibility.

For information on responding to privacy incidents see Chapter 15: Privacy incidents.

Review your complaints process

Your privacy complaints process should be reviewed regularly to ensure it remains fit for purpose. This is an activity you can add to your privacy officer's workplan.

Responding to privacy complaints

How you respond to a concern, or a complaint can have a significant impact on the experience of the complainant, and the resolution of the complaint.

When responding to a privacy complaint you should take the following steps:

1. Acknowledge the complaint.
2. Listen to the complainant.
3. Investigate the issues raised by the complainant.
4. Try to resolve the issues.
5. Rebuild the relationship.

For more information about these steps see our guide: Office of the Privacy Commissioner | Handling privacy complaints: a step-by-step guide.

Consider Tikanga

Incorporating tikanga into your complaints management process can be a powerful tool to help manage privacy concerns and complaints in a mana enhancing way.

A tikanga based approach to managing privacy concerns and complaints can help encourage parties to focus on communication and interaction during the process rather than just the outcome of the process.

Tikanga that can be readily incorporated into the way you manage complaints include:

- Kanohi ki te kanohi – where possible meet with the complaint in person.
- Whanaungatanga – spend some time getting to know each other before you get into discussions about the complainant's concerns.
- Manakitanga – encourage people to share their story, actively listen and build respectful relationships.

Additional guidance

For more guidance on how to respond to privacy complaints see our Poupou Matatapu guidance on responding to complaints well: Office of the Privacy Commissioner | Responding to requests and complaints well

The Ministry of Education also has guidance for schools and ECE services about managing general complaints:

- Schools: Dealing with complaints.
- ECE Services: Guidance For Developing A Complaints Policy.

What happens when the Privacy Commissioner receives a complaint?

A complainant (including a learner or their representative) must have attempted to resolve their issues with you before they can make a complaint to the Privacy Commissioner.

When a complaint is made to the Privacy Commissioner, the Commissioner will decide on whether to investigate the complaint and work to resolve the complaint in a way that is acceptable to both parties. The purpose of the investigation is to determine which principles of the Privacy Act may have been breached and how.

The Commissioner cannot investigate every complaint. The Commissioner is generally obliged to review an agency's response to access and correction requests but will triage other complaints from individuals to focus on cases where harm has occurred as a result of a breach of an Information Privacy Principle (IPP).

Where a decision to investigate is made, the Privacy Commissioner will contact both you and the complainant and advise that an investigation is commencing.

Investigations are conducted by talking to the parties concerned in person, by phone, email or in writing. You may also be asked to provide documents and information

relevant to the investigation, if this is the case you must provide the documents and information requested.

Additional Guidance

For more information about how the Privacy Commissioner manages privacy complaints see:

- Office of the Privacy Commissioner | Responding to requests and complaints well.
- Office of the Privacy Commissioner | Complaint Handling Policy.
- 2024 Decision Guide.

Privacy incidents

The Privacy Act requires certain types of breaches to be notified to the Privacy Commissioner and (nearly always) to affected people. Failure to notify the Commissioner of these types of breaches is an offence, so it's important for education providers to be aware of their responsibilities.

Sometimes, a breach may not meet the threshold to be notifiable. However, it's still important to track how many privacy incidents you have and to take them seriously. They can be useful indicators of problems that you have to fix to avoid causing harm in future.

Everyone understands that mistakes can happen, even when people are careful. If you cause, discover, or are informed about a privacy incident in your education agency, tell your privacy officer straight away. The privacy officer can help to limit any harm that might happen to affected people. They will know whether the incident is a notifiable breach and can liaise with the Privacy Commissioner and take any other steps that are needed to manage the incident. They can also help to fix things so that the problem doesn't happen again.

What is a notifiable privacy breach?

A notifiable privacy breach occurs when personal information you hold is:

- accessed, disclosed, altered, lost or destroyed accidentally or without authorisation **or** cannot be accessed by you on a temporary or permanent basis (e.g. encrypted by ransomware)
  and
- the action has caused or is likely to cause **serious harm** to affected people.

When a notifiable privacy breach is identified, you **must notify** the Privacy Commissioner and any affected people as soon as you are practically able to.

Examples of notifiable privacy breaches may include:

- Computers, removable storage devices, or documents containing personal information about learners being misplaced or stolen.
- Hardware being thrown away, recycled, sold, or returned to leasing companies without personal information about learners being removed first.
- Personal information about a learner being accessed by an unauthorised third party, for example, a hacker deploying malware or gaining login credentials via a phishing email.
- Losing the ability to access learners' personal information on learner or education management systems, for example, a security patch that fails and allows the system to be corrupted.
- Breaches of third-party providers who collect, process or store learner information on your behalf e.g. survey tools, student management systems, case management systems.
- Employees accessing personal information without a proper purpose (known as employee browsing) or a permission (system) error that allows a staff member to access a learner's personal information that their role would not normally allow access to.
- Sharing personal information about a learner inappropriately, for example:
    - ad hoc watercooler gossip about a learner
    - oversharing personal information about a learner at multi-agency meetings
    - sharing a learner's photos or videos without consent or other legal authority
    - entering a learner's personal information into online apps and tools that do not have adequate privacy protections.
- Information about a learner (including a postal address, email address, or mobile phone number) being sent to the wrong recipient.

- Information about a learner being accidentally sent to others. For example, sending on an email chain, failing to use ‘blind copy’ (bcc) on an email to multiple recipients, or attaching the wrong document to an email.
- Information about other learners visible to parents during a parent teacher interview.
- Unauthorised alteration of a learner’s personal information either intentional or accidental.
- A learner’s sensitive personal information being accessed by an unauthorised person and posted publicly online.
- Permanently losing the ability to access learners’ personal information on learner or education management systems due to a ransomware attack.

This is not an exhaustive list. These examples will only be considered notifiable breaches where serious harm has been caused or is likely to be caused.

Also, if a notifiable breach occurs, it doesn’t necessarily mean that you’ve done something wrong (e.g. you have sufficient security safeguards in place, but you are subject to a cybersecurity attack). But it does need to be properly dealt with, to prevent people from suffering additional harm.

Detailed information about managing a privacy breach can be found in our notifiable privacy breach management guidance: Office of the Privacy Commissioner | Breach Management.

What happens if a breach isn’t notifiable?

As you can see from the description, a notifiable breach doesn’t include things like failures to deal with access requests properly, using inaccurate information, or collecting more information than necessary.

These types of breaches aren’t notifiable, but they are still serious, and you need to manage them effectively.

Examples include:

- Not informing a learner (or their parents where appropriate) about a collection of their personal information.
- Retaining a learner's identity documentation longer than is necessary.
- Collection of personal information that unreasonably intrudes on a learner's personal affairs.
- Not taking reasonable steps to ensure personal information about a learner is accurate, up to date, relevant, complete and not misleading before you use or share it.
- Recording a meeting with a learner without their knowledge or authorisation.

It is important to have processes in place to identify and deal with breaches that aren't notifiable. Having clear and accessible processes in place enables you to deal with issue and fix the problem quickly.

Learners and their parents can make a complaint to the Privacy Commissioner if they believe you have acted in a way that has breached their privacy.

For more information about managing privacy complaints see Chapter 14: Managing privacy complaints.

What is a near miss?

A near miss is when an incident occurs but doesn't result in a privacy breach. Near misses can highlight problems with your security safeguards that may require review or attention.

Examples include:

- You respond to an email request for information about a learner but send that information to the wrong email address. However, the email address is wrongly spelt, and the email bounces back as undelivered.

- You discover a website vulnerability that exposes a learner's personal information but are confident that no other website user has seen the information.
- A CCTV camera is installed in the entrance way of an ECE service. While testing the camera it is discovered that the audio function is enabled. The ECE service manager disables the audio function before any private conversations of learners, parents or staff are captured.
- You are in an online meeting to discuss a learner and their learning support needs and realise that the AI transcription functionality is activated. You are able to turn the transcription functionality off before any personal information about the learner is discussed.

Managing privacy incidents

Managing privacy incidents well ensures any harm that may occur is minimised. It also helps to build trust with your learners and their parents, so that on the occasions when mistakes have happened, you will take timely and effective action to fix the problem.

Where you are informed about a privacy incident by another person (e.g. a learner or a parent), you should let them know how you are going to manage the incident. Report back to them. If they are not satisfied with the response, then let them know they can make a complaint. When you have received a complaint about a near miss or privacy breach, you should manage the complaint by following your privacy complaints process.

For more information about privacy complaints see Chapter 14: Managing privacy complaints.

Key steps

When a privacy incident has been identified, tell your privacy officer immediately. Then work with the privacy officer as necessary to take the following key steps:

1. **Contain** the breach to reduce any harm that the privacy breach has or might cause.
2. **Assess** for potential harm caused or likely to be cause by the privacy breach.
3. **Notify** if the breach has or is likely to cause serious harm (notifiable privacy breach).
4. **Reflect** on what caused the breach and make improvements to systems, process or practices where required.

More information about these four steps can be found in our notifiable privacy breach management guidance: Office of the Privacy Commissioner | Breach Management.

Notify the Privacy Commissioner

You are required to notify the Privacy Commissioner of any notifiable breaches. Use the notification tool on the Privacy Commissioner's website.

You are not required to notify the Privacy Commissioner or affected learners of near misses.

We recommend that you record your reasons for determining that a breach is or is not notifiable in your privacy incident register.

Notifying learners under 16 years of age of notifiable privacy breach

You are generally required to notify affected people about notifiable breaches so that they can take steps to protect themselves (e.g. protecting their safety, watching for unexpected emails, alerting their bank, or protecting against identity theft).

However, you are not required to notify an affected learner of a notifiable privacy breach if:

- the learner is under the age of 16
  and
- you believe notification would be contrary to that learner's interests.

If you consider that notifying learners under the age of 16 would be contrary to their interests you **must** consider whether it would be appropriate (considering the circumstances of both the learner and the privacy breach), to notify a representative of the learner instead.

A parent or guardian of a learner who is under the age of 16 is a representative for the purposes of notifying a privacy breach. Where a learner is over the age of 16, you will need to comply with the notification requirements set out in the Privacy Act.

This definition of representative only applies to privacy breaches. It does not apply to determining whether a requestor is a representative for the purposes of an IPP6 access request.

Detailed information about the things you need to notify affected learners about can be found in our general privacy breach management guidance: Office of the Privacy Commissioner | Breach Management.

Example - Decision to not notify affected learners under 16 years (ECE service)

An ECE service experiences a cybersecurity incident where a list of all learners attending the service, including their names, birth date, National Student Number, and health conditions, are made available to the public. No information about the learners' parents is disclosed. The ECE service manager assesses the breach. The ECE service manager determines that it is a notifiable breach as personal information about the learners has been accessed and disclosed intentionally by an

unknown third party, some of it sensitive, and it is likely to cause the learners' serious harm.

Does the ECE service manager need to notify the affected learners?

The ECE service manager is not required to notify the learners if they are under 16 years of age and it would be contrary to the learner's interests. In this case, due to the age of the learners, it would be considered contrary to their interests as they are too young to read and understand the notification or take any action to mitigate the harm caused by the breach.

Having determined that notification would be contrary to the learners' interests, the ECE service manager must then consider whether it is appropriate to notify the learners' representatives – their parents. As part of this consideration, the ECE service manager must consider the circumstances of the both the learner and the privacy breach.

Given the learners' age, lack of ability to take any action to mitigate the harms caused by the breach, and the sensitivity of the information disclosed, it would be appropriate for the ECE service manager to notify the learners' parents.

If the parents' personal information has been disclosed, the ECE service manager would need to consider whether the breach had or was likely to cause serious harm to the parents affected, and if so, the parents would also need to be notified about the breach of their own personal information.

Example - Ensuring learners (or their representatives) are notified appropriately – develop a privacy breach notification template

Managing a privacy breach can be challenging. To help ensure you notify learners (or their representatives) quickly and appropriately, it can be helpful to have a privacy breach notification template form ready to go when a breach occurs.

A privacy breach notification template should enable the following information to be provided to the learner (or their representative):

- Information about the incident, such as the date it occurred, a description of the information that was disclosed and what hasn't been disclosed.
- Who might be in possession of their personal information (you shouldn't include any information that could identify that person or body, unless considered necessary to prevent or lessen a serious threat to the life or health of an individual).
- What is being done to control or reduce the harm. This could include general information about the potential types of harm that could be caused, given the personal information involved.
- What you are doing to help people and what steps the affected people can take to protect themselves (e.g. changing passwords, monitoring suspicious activity, being aware of potential scams such as phishing emails that often follow a privacy breach).
- A key contact person for enquiries and complaints – you may want to also consider adding information to your website or parent communication portal.
- Confirmation that the Office of the Privacy Commissioner has been notified.
- That they can make a complaint to the Office of the Privacy Commissioner and information on how to make a complaint.
- If applicable, that the notification is being made to the representative due to the affected learner being under the age of 16.

Privacy incident management tools

A privacy incident management plan and a privacy incident register are useful tools to help you manage privacy incidents.

Privacy incident management plan

You should have a privacy incident plan that sets out what you will do, how you will do it and who is responsible for those actions. A privacy incident management plan should cover processes for managing near misses, privacy breaches and notifiable privacy breaches.

For a privacy incident management plan to be effective, everyone needs to know:

- about the privacy breach management plan and they can find it
- the processes they are required follow when they discover, or are informed about, a privacy incident
- what their role and responsibilities are when a privacy incident occurs.

Detailed information about what to include in your privacy incident management plan can be found in our general privacy breach management guidance: Office of the Privacy Commissioner | Breach Management.

Privacy incident register

All privacy incidents (both notifiable breaches and near misses) should also be recorded in a privacy incident register.

Creating and implementing a privacy incident register enables governance members to be aware and have oversight of the number and types of privacy incidents (and any common themes or trends). It provides an opportunity to review privacy processes and practices and make improvements where necessary.

A privacy incident register should include:

- the date the incident occurred
- the date the incident was discovered
- the type of incident (breach or near miss)

- the action that led to the incident e.g. unauthorised access, use, sharing or loss of personal information
- the underlying cause of the incident
- whether the incident was accidental or intentional
- scale of the incident (e.g. how many learners or records were affected by the breach)
- sensitivity of the information that was subject to the incident
- who accessed the personal information (if known)
- nature of the harm to the learner
- if a breach, whether it was notifiable
- if a notifiable breach, when the Privacy Commissioner and affected people were notified
- if it was not notifiable, the reasons why the breach is not notifiable
- the response to the incident.

Digital technologies

Technology, including digital products and services, plays a key role in the education sector.

This includes tools for delivering education services (e.g. online learning platforms, virtual classrooms), undertaking assessments, parent communication tools, to managing administration and operations.

Understanding when and how to use technology to deliver educational outcomes is becoming a critical skill for education sector workers.

Digital technologies offer many benefits including enhanced learner opportunities, increased engagement, and greater access to information and resources. The use of digital technologies helps to create mature digital citizens, preparing our learners for the next stages of their professional and personal development. Technology also provides insights into the health of our education system and helps ensure learners are on the right path by identifying barriers to learning early.

Digital technologies can be transformative and provide benefits to both those working with learners and the learner themselves. We can now curate more data and information about learners than ever before, but this has the potential to put learners' privacy at risk. Just because a digital technology has benefit for an education provider doesn't mean its use will be in the best interests of the learner.

Education providers need to critically evaluate and understand what the introduction of digital technology means for your learners' privacy.

Privacy risks associated with digital technology

Digital technologies that collect, use, store or share a learner's personal information can create privacy risks. Knowing and understanding the privacy risks associated with digital technologies can help you identify and manage those risks and ensure a learner's personal information is protected.

The following table identifies some of the privacy risks associated with digital technologies, including technologies that use artificial intelligence:

Privacy Risk	Example
Overcollection of personal data and information	• Use of cookies. • Browser and location tracking - mobile based apps and tools may monitor a learner's activities in and outside of the education environment and in contexts unrelated to education-related activities. • Remote learning, tutoring or proctoring tools may continually collect audio and visual information about learners in their homes or private spaces. • Web-based learning management systems may collect every click or page transition a learner makes, or contextual information such as date and time of those actions.
Unauthorised use and disclosure of personal data and information	• Digital technology vendors using learners' personal data, information and content to train Generative AI models (e.g. Chat GPT) or algorithms. • Sharing or sale of a learner's data and information to third parties. • Creation of and reliance on out of date, inaccurate or biased content to make decisions, including automated decisions, predictions or inferences about learners.

	• Creation of psychological profiles and predictions of academic performance and achievement.
	• Chatbots used as teaching tools or to provide education and learning support in classrooms may:
	  ○ interact with learners in ways that are not appropriate
	  ○ encourage the learner to disclose personal information they may not otherwise share
	  ○ infer and then use personal information that the learner did not intend to disclose.
	• Ability to inappropriately link a learner's data and information to other data and information and over time build an in-depth profile of a learner across different platforms.
	• Digital technology provider disclosing a learner's data and information to third parties without the learner's (or their parents) knowledge or consent.
	• Personal information entered into a digital technology may be made available to other users of that technology or other service providers (this is particularly relevant with free digital technologies).

Storage and security	• Insecure storage of learner data and information making it easier for unauthorised individuals to gain access to learner's data and information. • Digital technology may not have sufficient security safeguards to keep learner data and information safe (e.g. no multi-factor authentication). • Learner information may be retained by the digital technology vendor longer than is necessary.

Accuracy, transparency and bias	• Outputs from digital technologies may not be accurate. • Lack of transparency and explainability around how the technology works, processes or discloses a learner's personal information. • Existing bias, inequities or errors within technology are amplified or lead to poor decisions.

Free digital technologies

Free, or free trial periods, of digital technology products or services can create more privacy risk. Digital technologies are usually offered free of charge when the vendor wants to use the data and information provided for its own purposes (e.g. improving the digital product, training the models operating behind the digital product, and the sale or sharing of the learner's data and information to third parties).

Free, or free trial periods, digital technology products or services might look attractive from a budget perspective, but they often have fewer privacy safeguards in place. Fewer privacy safeguards can expose a learner's personal information to a higher degree of risk including unauthorised access, use or disclosure.

Education providers are responsible for making sure digital technologies introduced into their environment are assessed, selected, implemented and used in a way that ensures learners personal information is protected and respected.

You should not solely rely on assurances from a technology vendor that its digital technology product is privacy protective. You need to undertake your own due diligence processes to ensure that the digital technology complies with the Privacy Act 2020.

Foundations for privacy protective digital technology

Foundations for privacy protective digital technology include:

- a digital technology policy
- an acceptable use policy
- a digital technology register.

Getting these basics right will set you up well for ensuring your digital technology complies with the Privacy Act 2020.

Develop and implement a digital technology policy

A digital technology policy is a set of guidelines and rules that govern the assessment, approval, and use of digital technologies. All digital technology decisions should be made following the digital technology policy.

The policy should cover:

- purpose of the policy
- who the policy applies to
- the digital technologies the policy applies to
- a statement on whether non-approved digital technologies can be used
- a statement that all digital technologies must protect and respect personal data and information and meet the privacy and security policy requirements
- the process to assess and select digital technologies
- the roles responsible for the assessment process
- the roles responsible for approving the implementation and use of digital technologies
- the requirement for all digital technologies to be recorded in a register
- the review cycle for digital technologies, and who is responsible for undertaking the review

- retention of learner data and information when a learner leaves the education provider or the digital technologies are no longer required, used, or a licence to use has expired
- a review period for the policy.

Your digital technology policy should be accessible to staff, learners and their parents. This transparency demonstrates that you will carefully consider the use of any new digital technology to ensure it is privacy protective which helps build trust and confidence in how you manage and protect personal information.

Develop and implement an acceptable use policy

An acceptable information technology (IT) and internet use policy is a set of guidelines and rules that govern the appropriate use of computers and digital devices, networks and the internet by learners and staff. An acceptable use policy sets expectations that help to protect your IT infrastructure and data and information from security threats and misuse.

Your acceptable IT and internet use policy can also refer to your digital technology policy and require digital technologies (e.g. software programmes, apps and other digital tools) to be approved before being used on work devices (e.g. computers, tablets, or phones).

The Ministry of Education guidance *Acceptable use guidelines at your school* provides more information about how to develop and maintain an acceptable use policy.

This guidance can also be used by and adapted for Early Childhood Education (ECE) services and service providers.

Develop and maintain a digital technology register

A digital technology register is a good way to maintain oversight of what's being used, help staff know what's allowed, and reduce the risk of unapproved digital technologies being introduced and used.

You can tailor your register to suit your needs, but at a minimum it should include:

- Product/Service name.
- Product/Service vendor name.
- Product/Service vendor contact.
- Product/Service purpose.
- Date procured.
- Licence expiry (if applicable).
- Personal information that can be entered into the product or service.
- Date privacy assessment completed.
- Outcome of privacy assessment.
- Date of Board/Management approval.
- Product/Service review date.

A digital technology register works best when new digital technology is added to it in a timely manner. It should also be reviewed regularly to make sure it's up to date. The requirement to add approved digital technology to the register, and the register review cycle should be included in your Digital Technology policy.

Example - Digital Technology Register

A technology register doesn't have to be complicated – a simple Excel spreadsheet will work:

Product/Service Name	Product/Service Vendor Name	Product/Service Vendor Contact	Product/Service Purpose	Date Implemented	Personal Information (Collected, Used, Stored and Shared)	Privacy Assessment Completed	Board/Management Approval	Licence Expiry	Review Date	Review Completed
Seesaw	Seesaw	John Smith 021 xxx-xxxxx	Parent Communication app	1/01/2025	* Learner name, age, class, progress and achievement information, atttendance, health information, photos and videos * Parent name, contact details	20/08/2024	1/01/2027	1/01/2027	1/01/2025	12/01/2025

Your digital technology register should be available to all staff so that they're aware that technology-based products and services have been assessed as safe to use. Making the register available to learners and their parents (e.g. through your privacy policy) is also a good way to be transparent about how you manage learners' personal information.

You could also add your digital technologies to an existing register (e.g. your asset register) to reduce the number of registers you need to review and maintain.

Ways you can make sure digital technology is privacy protective

There are a few key things you can do to help make sure digital technologies protect your learners' privacy.

Have a clear purpose for the digital technology

Understanding the problem that you're trying to solve or outcome you are wanting to achieve will help you:

- workout whether a digital technology is the right solution
- identify digital technologies that are fit for purpose and privacy protective
- ensure the digital technology will meet your and your learner's needs.

Do your due diligence before you select your digital technology

Understanding how the digital technology works, how it collects, uses, stores and shares personal data and information, and what access the vendor may have, is critical to ensuring the digital technology is privacy protective. Due diligence means

going beyond the sales pitch – you need to do your own research to ensure the digital technology will protect the privacy of your learners.

Use our digital technology due diligence checklist.

Just because another education provider is using a digital technology doesn't mean it is privacy protective. You need to undertake your own due diligence processes to ensure that the digital technology complies with the Privacy Act 2020. Talking to other users of the digital technology can, however, help you identify potential privacy issues.

If you are in doubt, contact the product or service vendor and ask them questions (using the checklist above). Often digital technology vendors will claim that their digital technology complies with privacy laws and international standards – don't be afraid to ask the vendor to provide independent assurance that their digital technology is in fact privacy protective.

Safer Technologies for Schools (ST4S) Framework

Safer Technologies for Schools (ST4S) is an initiative led, in New Zealand, by the Ministry of Education. ST4S supports schools to choose privacy protective digital technology by assessing digital technologies against privacy and security standards.

The ST4S initiative focuses on digital technologies. Digital technologies that carry an ST4S badge have been assessed against minimum privacy and security standards required to protect learner privacy.

ST4S provides detailed reports that contain information about the digital technology to help you make an informed decisions around purchasing and implementation. The ST4S reports contain information about:

- what personal information the product or service collects, and how it uses that information
- how well the product or service performs against privacy and security standards

- recommendations on how to reduce privacy or security risks.

ST4S reports don't endorse digital technologies, but they can help you decide whether a particular technology prioritises learner privacy and security and meets the specific needs of you and your learners.

If you are looking at a digital technology that has not yet been assessed by the ST4S initiative, you can let the Ministry of Education know and they will encourage the digital technology vendor to complete the assessment.

For more detailed information about ST4S including how you can access the reports see:

- Choosing safer technologies for schools and kura - Ministry of Education.
- Safer Technology 4 Schools (Australia).

The information you obtain through your due diligence process, including information contained in the ST4S reports, will then help you complete an assessment of any privacy risks associated with the use of the digital technology.

Assess the digital technology for privacy risks

Privacy assessments play a crucial role in ensuring the privacy (and security) of personal information in the rapidly evolving landscape of digital technologies.

Completing a privacy assessment will help:

- ensure the collection, use, storage and sharing of information by the digital technology is compliant with the Privacy Act
- identify privacy risks early and mitigate potential privacy risks that may arise from the implementation of new digital technologies, reducing the risk of privacy breaches or other privacy related incidents
- decision makers make informed decisions about how to handle learners' personal information in privacy protective and respectful ways

- communicate your protective privacy and safety processes to your learner community
- build trust and confidence in the way you manage learners' personal information.

Completing a privacy assessment may feel too hard, too time consuming or you may believe you don't have the necessary knowledge to complete the assessment properly. However, time spent ensuring your learner's personal data and information is protected before you introduce new digital technologies, will:

- help you select and implement digital technologies that prioritise protecting your learner's privacy
- ensure your use of digital technology is in the best interests of your learners
- save significant time and resources later if there is a privacy breach, a complaint or other privacy related incident.

We have developed tools and guidance to help you complete a privacy assessment effectively and efficiently: Office of the Privacy Commissioner | Privacy Impact Assessments.

Implement and manage identified privacy risks

Having completed your due diligence and undertaken a privacy assessment, you will have identified any privacy risks associated with the use of the digital technology.

Before implementing the digital technology, you will need to develop appropriate business processes or controls to ensure those privacy risks are mitigated. These processes or controls could include:

- access control processes:
  - who can access what information and for what purpose
  - who approves access to the information
  - responsibility of users to only access and use information for approved purposes
  - offboarding users who no longer require access.

- consent processes for collecting, using or sharing a learner's information using the digital technology (e.g. collection and use of photos or videos)
- integration restrictions with other digital technologies or business systems to ensure the digital technology can't access learner information that it doesn't need
- restrictions around the use of personal devices to access the digital technology
- staff training requirements.

Identifying and managing privacy risks is not a 'one and done' thing. For example, you shouldn't leave off-boarding users of digital technologies until your review of the digital technology. Staff who no longer require access to the digital technology should be offboarded in a timely manner to manage the risk of unauthorised access to a learner's personal information.

Review your digital technologies to ensure they remain fit for purpose

It is important to review your digital technologies to ensure they remain fit for purpose, continue to deliver benefits for you, your learners and their parents, and are still privacy protective. This is where the digital technologies register is vital – all your digital technologies are recorded in one place.

Knowing when a digital technology is due for renewal enables you to check that the technology is still fit or purpose, and the privacy and security safeguards are still protecting your learner's personal information appropriately. It also helps you to identify learners that no longer attend your school, ECE service or service and remove (e.g. delete or archive) their personal data and information from the digital technology.

Knowing when a digital technology licence or subscription is due to expire means you can plan for the recovery or disposal of any personal information that may be held by the digital technology vendor.

Things you can consider as part of your review may include:

- Has the digital technology been updated, the functionality changed or has new functionality been added (e.g. new AI functionality was added)? Has the update or new functionality created new privacy risks for your learner's personal information (e.g. changed previously applied privacy settings)?
- Has the digital technology vendor updated their privacy policy or terms and conditions of use? Do these changes create new privacy risks for your learner's personal information?
- Has your use of the digital technology changed? Are you using the technology for new purposes? If so, do these new purposes create new privacy risks for your learner's personal information?
- Have all security updates been completed as required?
- Are your business processes for using the digital technology still fit for purpose? Do you need to update these processes?
- Have you received any complaints about the use of the digital technology or have any privacy breaches occurred as a result of using the digital technology?
- If you have stopped using any digital technologies has all your learner's personal information been retained or disposed of appropriately?

Staff training

It's important that people working for an education provider know what digital technology is approved for use, what personal information can be entered into digital technologies available, and the processes for seeking approval for new digital technology.

Staff training is a good way to make sure everyone knows what they can use, what they can use it for, and how they can ensure learner's personal information is protected when they are using digital technologies.

Using artificial intelligence

Artificial intelligence is a technology that can perform tasks typically undertaken by people such as basic reasoning, learning, decision-making and perception. Artificial intelligence technologies are no different from other digital technologies - your use of it must comply with the Privacy Act and protect your learners' personal information.

Examples of AI use in education settings include:

- Large language models (e.g. ChatGPT).
- Instructional materials (e.g. lesson plan generation, study material generation, multimodal instruction, explanation generation).
- Assessment and feedback tools (e.g. AI-assisted marking, feedback on learner work, quiz and question generation, learner progress tracking).
- Teacher practice support (e.g. analysis of learner data, academic integrity, administrative tools to free teacher time).
- Teacher professional learning (e.g. instructional learning, knowledge refresh, classroom management).
- Learner support (e.g. AI-enhanced tutoring, academic, college and career advice, support for neurodivergent learners and learners with learning support needs, homework assistance).
- Social tools (e.g. interest-based groups and networks, class discussion facilitation, small group facilitation, peer tutoring).

Read more detailed information about education specific AI use cases..

Before introducing artificial intelligence technologies, the purported benefits should always be carefully considered against the best interests of your learners, including their privacy rights.

For more information on artificial intelligence and the Privacy Act 2020 see our guidance: Office of the Privacy Commissioner | Artificial Intelligence and the Information Privacy Principles.

For more detailed guidance on the use of generative artificial intelligence in schools more generally see: Generative AI - Ministry of Education.

Privacy protective digital technology in practice

This section provides some examples of how to ensure you implement and use privacy protective digital technology in the education sector.

Example - New online tool to support a learning activity

A teacher has found an online tool that they believe will help their year 7 learners with learning maths. It's a fun interactive tool, which is free to use. The online tool works by uploading lesson plans, and learner details such as name, age and their math progress. It then then provides each learner with activities and games for specific maths skills across various levels of difficulty. The online tool analyses the learner's answers and time taken to complete activities and provides this insight data back to the teacher.

Should the teacher download and use the online tool?

No, they shouldn't without first understanding more about the online tool and the privacy impacts.

Given the online tool collects and uses learner personal information, there will be privacy risks associated with it. If the online tool is free to download and use, it is unlikely that the tool's privacy and security safeguards will be sufficient to ensure the learner's personal information is protected. It may also be impossible to delete learner information from the tool when the tool is no longer used, or the learner moves classrooms or schools. There is also a high risk that the online tool vendor

will be able to use the learner's personal information for its own purposes (e.g. targeted advertising, sale of information to third parties).

Before using digital technologies, you should first check your education provider has a digital technology policy. If they do, you should follow the process for making a request to use new digital technologies. If your education provider doesn't have a digital technology policy or process for approving new digital technologies, you should always assess the digital technology for privacy risks and only implement and use digital technologies if you are satisfied that the requirements of the Privacy Act 2020 are met and your learners' 'personal information will be protected.

Example - Assessing privacy risks of technology products and services

The parent communication app licence that an ECE service uses is due to expire. The ECE service manager wants to move to a new parent communication app that can be integrated into the learner management platform used by the ECE service. This functionality means that parents can be informed about the activities their child is doing while at the ECE service, and progress their child is making. The app vendor's webpage states that the app complies with the New Zealand Privacy Act 2020.

What should the ECE Service manager do to ensure that the new parental communication app protects personal information appropriately?

The ECE Service manager shouldn't rely on the app vendor's statement that the app complies with the Privacy Act 2020. The ECE service manager is responsible for ensuring personal information is managed appropriately, so they will need to make that determination themselves.

To do that, the ECE service manager should first obtain sufficient information about the app so that they can complete a privacy assessment. A good place to start is the app's privacy policy which can usually be found on the vendor's website. The privacy

policy should provide information about how it complies with the Privacy Act 2020, including:

- what personal information the app collects, how the app uses that information, and who the information may be shared with and for what purposes
- the privacy and security features embedded into the app and how those features protect personal information
- how long the personal information is stored and whether the personal information can be deleted when the app is no longer required by the ECE service, or when a learner moves to another education provider
- whether the vendor has access to information held in the learner management system when the app is integrated
- the rights and responsibilities for the parties over the content uploaded and created in the app.

With this information, the ECE service manager can assess the app against the Information Privacy Principles (IPPs) in the Privacy Act 2020. This assessment will identify any privacy risks associated with the use of the app and enable the ECE service manager to identify additional business processes or controls that may be required to mitigate those risks. The ECE service manager can use the privacy impact assessment resources and tools to help them successfully complete the privacy assessment: Office of the Privacy Commissioner | Privacy Impact Assessments.

Where the privacy assessment results in a high privacy risk, and those risks cannot be mitigated, the app should not be approved for use. Where the privacy assessment results in a low privacy risk, where any residual risks can be mitigated, the ECE service manager could approve the app for use within the ECE service.

Once the app has been approved for use, the ECE service manager will need to think about what business processes are required to ensure the app is implemented appropriately and used in a privacy protective way, including:

- how the app will integrate with existing business systems, and ensuring the app can't access learner information it doesn't need to function
- consent processes for collecting, using or sharing learners' personal information using the app (e.g. collection and use of photos or videos)
- log in processes and access controls to ensure only authorised staff can input, access, use or share personal information within the app
- restrictions around staff using personal devices to access and use the app
- staff training requirements to ensure all staff know how to use the app, what personal information can be entered into the app, and how that information can be used.

When implementing new digital technologies, it is always a good idea to let your learners, and their parents know. The ECE service manager can do this by creating a privacy statement specific to the app and provide the privacy statement to the learner's parents. The ECE service manager should also update the ECE service's privacy policy, and its digital technology register if it has one.

Example - Can I put a learner's personal information into an AI tool such as ChatGPT?

As a starting point, personal information should never be entered into free versions of AI tools as the privacy and security safeguards associated with free or trial versions are often lacking, exposing learner's personal information to significant risks.

Even when AI tools have been approved for use, you should always take a cautious approach to entering a learner's personal information into an AI tool.

Information entered into AI tools is often retained and used to train the underlying model. Once the information is entered it is almost impossible to retrieve it or delete it. This can have both short- and long-term impacts for the learner.

Example - Can I use an AI assistant to help manage meetings and take minutes?

Before using an AI assistant, you should do your due diligence and assess the AI assistant for privacy risks.

Personal information should never be entered into free versions of AI assistant tools. Even if an AI assistant has been approved for use, you should always take a cautious approach to collecting, using or sharing a learner's personal information when an AI assistant is operating.

If an AI assistant has been approved for use, you should always let people know that it is operating in the background and what it is doing (e.g. sending meeting invites, recording meetings, taking meeting notes). That way meeting participants can be mindful about what information about learners they share within the meeting and can choose to turn their cameras off if they don't want their image captured by the AI assistant.

While AI assistants can provide administrative efficiency benefits, they also have the capability to process large amounts of personal information which is used to improve user experience and functionality. As such, use of these AI assistants can create privacy risks.

These privacy risks include:

- unintended collection of personal information
- unauthorised use of personal information
- unauthorised disclosure of personal information
- lack of transparency around how AI assistants collect, use, store or share personal information
- insufficient security controls increasing the risk of unauthorised access to a learner's personal information.

For example, multiple privacy breaches occurred when an AI assistant was used by a meeting participant to record and create notes of the meeting. The meeting included discussion about individual learners and their learning support needs.

The AI assistant was operating in the background and other meeting participants were not aware that it was recording the meeting. After the meeting, the AI assistant proactively emailed the meeting notes it had created to everyone who received an invite to the meeting including those that had not attended the meeting.

Under the terms and conditions of the AI assistant, the recording and the notes created from that recording could be retained and used by the AI assistant vendor to train and improve its AI model.

Unique identifiers

A unique identifier is defined as an identifier, other than a person's name, that uniquely identifies that person. Special care should be taken when collecting, using or sharing unique identifiers.

Relevant information privacy principle

The Privacy Act sets out rules for the creation, use and protection of unique identifiers.

The relevant Information Privacy Principle (IPP) is:

Principle 13: Unique Identifiers

An education provider may assign a unique identifier to a learner for use in its operations only if that identifier is necessary to enable the education provider to carry out its functions.

An education provider must take steps to ensure that:

- a unique identifier is assigned only to a person whose identity is clearly established
  and
- the risk of misuse of a unique identifier is minimised.

Common unique identifiers in education sector

Common unique identifiers include:

- National Student Number (NSN).
- National Health Index (NHI).

- Social Welfare Number (SWN).
- Inland Revenue Number (IR Number).

A person cannot be requested to provide a unique identifier assigned to them unless that disclosure is for one of the purposes for which the unique identifier was assigned or is directly related to one of those purposes.

For example, an education provider cannot request the IR Number of a learner or their parents (unless the learner or parent is employed by the education provider). However, where a school employs a counsellor or nurse it may be appropriate to request the learner's NHI so that health and disability support information collected are attached to the correct learner in relevant health databases.

National Student Number (NSN)

The National Student Number (NSN) is a unique identifier given to every learner as a digital identity. Assignment and use of NSNs is governed by Education and Training Act 2020.

For more information about the NSN, and who is authorised to use the NSN for specified purposes, see:

- About National Student Numbers - Ministry of Education.
- Education (National Student Numbers) Notice (No. 2) 2024 - New Zealand Gazette.

From a Privacy Act perspective, the NSN is personal information about a learner and may help to identify a learner. For example, removing a learner's name and replacing it with their NSN, will not mean the learner is not identifiable – the information will still be attributable to an individual. Other information contained in the document (for example, information contained in a learning support register) may also be sufficient to identify them.