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.