Privacy Commissioner
Te Mana Mātāpono Matatapu

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.