Building Capability and Awareness

Overview

Robust and effective training is an important component of building privacy capability, as well as a driver of a privacy mature culture within your organisation.

While some fundamentals will apply across all organisations, there's also specific areas where you might need bespoke training.

This pou provides guidance on:

- Creating a privacy training programme – what do you need to consider?
- Types and methods of training.
- Promoting and building privacy awareness.

Who is this for?

Your privacy function and those with a responsibility for planning and/or delivering privacy training.

Key objectives of the Building Capability and Awareness pou

What would we expect to see?

- Organisation has a role list with privacy training needs identified and training records for employees.
- Appropriately trained people are available to deliver the training.
- Training is received as part of induction and/or prior to gaining system access.
- Trends identified in reporting of breaches and near misses are used to uplift capability in areas that need it. For example, via training, refreshers, or targeted sessions.

Creating a privacy training programme

Good privacy is everyone's responsibility. Individuals in your organisation should have a basic understanding of what privacy is and how to spot and escalate privacy issues. It's important that everyone in your organisation receives, at a minimum, some basic training on their responsibilities when it comes to privacy. However, not everyone will require the same level of training, depending on their day-to-day duties and whether dealing with personal information is integral to their role.

Your privacy training programme should cover how to appropriately collect, use, protect, disclose, and dispose of personal information, and should be supported by documented policies and procedures.

A good privacy training programme is one that:

- Is tailored and targeted to the different roles and responsibilities in your organisation.

- Is accessible to all roles in your organisation.
- Provides for ongoing engagement refreshers.

The aim of your privacy training programme is not to make everyone an expert in the legislation or even privacy generally. It is to provide your staff at every level with the knowledge and skills to apply privacy concepts relevant to their work and contribute to good privacy practice, as well as understanding your organisation's expectations. It's also a way to ensure that staff know where to go for more detailed information if they need it, and who to escalate privacy issues, requests, or breaches to.

There are some key considerations to make when setting up your privacy training programme.

Identify your target audiences:

- What are the privacy risks associated with each employee group in each area of the organisation?
- What does each group need to know? For example, don't give people training that they don't need for their role. Make the training specific.
- Who will deliver the training, and have they been appropriately trained or given appropriate materials?

Set a timeframe:

- Will staff be trained as part of induction and onboarding when they start their role?
- Is there specific training that certain staff will need before they have access to systems containing sensitive personal information?
- When will you require staff to undergo a training refresher? E.g. every six months, annually, or when/if their roles and responsibilities change (you might use a combination of all three depending on the needs of your different employee groups).

Maintain training records:

- Keep records of training materials and details of who receives the training, ensuring only the minimum amount of personal information is collected.
- Can you easily confirm which staff have received training (including refreshers), and when?
- Do you have a record of which staff or employee groups require targeted training specific to their role, and when this scheduled?

Monitor your training programme:

- Is there a way for staff to provide feedback on their training? E.g. post-training survey or feedback form.
- Staff surveys – these can be a useful tool to assess the effectiveness of your training programme. For example, asking a series of privacy-based questions to test staff understanding.

Train your trainer

As part of creating your privacy training programme, you will need to ensure your organisation has trained people available to deliver training to staff.

Designing and delivering privacy training will likely be the responsibility of your privacy function, so it's important that they also receive regular training and opportunities for professional development.

Investing in the development of your privacy function ensures that they have the skills needed to deliver training, are clear on their responsibilities, and are providing staff with relevant and up to date privacy training.

This could include sending your privacy function to external specialised training days or qualification courses, privacy workshops or forums, and ensuring they have time dedicated to regular professional development.

Methods of training

While there may be a place for a formal, classroom-based privacy training programme, it is not the only method you can use to build capability in your organisation.

Formal:

- Classroom training e.g. during formal induction to a job.
- Presentations.
- Workshops and seminars.
- External qualifications or micro-credentials e.g. privacy officer training.

E-learning:

- OPC offers free online training covering a variety of privacy topics.

  OPC e-learning modules:

  - Privacy 101
  - Privacy ABC
  - Privacy Act 2020
  - Privacy breach reporting
- There are other privacy e-learning options available, though these can come at a cost. Some organisations choose to develop their own privacy e-learning modules that are delivered via their learning management system.

On the job:

- Coaching or 'buddying' by an experienced coworker or trainer.
- Targeted discussions as part of team meetings.
- Shadowing a coworker or observing a process or task being completed.
- System or application specific training.
- Drop-in sessions run by the privacy function.

Values based training:

An effective way to make your training, and privacy programme in general, more relevant and engaging for your staff is to make meaningful links to your organisation's values and culture. This can show how good privacy practice supports success in meeting organisational values, which staff are often measured against during performance assessments.

For example, if one of your values is being customer-centric and people focused, think about how your privacy practices can reflect this, and communicate it to your staff in their training.

Bringing your staff together for training can be a great opportunity to build your privacy and wider organisational culture.

Promoting and building privacy awareness

Privacy training and awareness are key to building and maintaining a privacy culture within your organisation. Privacy awareness activities should reinforce your training programme through regular reminders.

Communications plan

Including privacy initiatives in your organisation's communications plan can be a useful way to deliver privacy messages. For example:

- Participating in campaigns such as Privacy Week, Cyber Awareness Week.
- Newsletters and the intranet – incorporating privacy messages into any newsletters your organisation sends out.
- Messages from your CEO or leadership team – this can act as a powerful tool to promote privacy awareness within your organisation, particularly if there are shortcomings that you want to communicate to the organisation, for example if you have spotted an increase in a particular type of breach.
- Inviting people to share real stories from their experiences with privacy breaches.
- Sharing insights from the organisation's privacy reporting – what's going well, uptake rates for privacy training, and lessons learned from incidents and near-misses.

Policies and procedures

Your policies and procedures should be readily accessible for all staff within your organisation. This is a critical part of building privacy capability and awareness.

Key questions to consider are:

- Can your staff easily find policies and procedures?
- Could your staff explain their role and responsibilities and how the policies and procedures help them?
- Are your policies and procedures simple, clear, and effective? If they aren't, staff are less likely to understand and therefore access and use them.

Some ways to achieve this include:

- Providing links to policies and procedures on your organisation's intranet, or equivalent (if you have one), or providing them in other formats e.g. hardcopy if necessary.
- Regularly informing staff when policies and procedures are updated.
- Using visual materials to emphasise key messages e.g. posters.
- Incorporate discussions about relevant aspects of policies into team meetings.

Visibility

Visual reminders are a simple but effective way to promote awareness around your organisation. These could include:

- Posters
- Booklets and flyers
- A Privacy 'hub' on your intranet or equivalent e.g. links to internal policies and procedures, privacy function contact information, links to external resources.

Keep in mind you don't have to create your own resources from scratch. Think about how you can leverage privacy resources from other authorities. For example, Office of the Privacy Commissioner, CERT NZ, Netsafe, etc.

Organisation examples

We've included some use cases based on fictional organisations to demonstrate each of the pou in practice. Read more about them in Introducing the Organisation Examples.

Large business – Fern Leaf

As a large organisation, staff at Fern Leaf must complete mandatory training when they join, with refreshers after one year of being at the organisation. To cater for the broad audience of staff, Fern Leaf's privacy training covers good privacy practice for collecting, using, storing and disclosing personal information. The materials try to engage the audience by not being too legalistic in tone and making it relatable to Fern Leaf's values of consumer first.

Completion of mandatory training is held by the HR team. However, the privacy team have identified that different areas of the business require different training. It has set up a dedicated training module for shop workers, with reference materials available to them. Team leaders also receive communications throughout the year to specifically share with their team members.

On the intranet, Fern Leaf has a form that staff can complete to provide feedback on the privacy training content. Feedback is regularly reviewed and changes to training made where possible.

Small business (charity) – Reach High

As a small organisation with a high privacy risk profile, Reach High recognises that it needs to develop a privacy training programme, but do so in a way that will not cost too much money. Because Reach High only has 15 staff, it can achieve this quite easily. The Director of Support Services gets external help to develop a set of privacy training materials for the three key functions of the organisation – counselling and mentoring, fundraising, and

employment (for people leaders). She delivers these workshops on an annual basis and to new staff when they join. She records staff completion in the Privacy Risk Register.

Start-up – Swiftstart NZ

Swiftstart NZ is a small organisation with limited resources to dedicate to privacy training but recognises that this is something that all staff need to understand. As a starting point, all staff complete OPC's Privacy 101 module and provide evidence of completion to the Operations Manager. New staff who join will be expected to complete the 101 module as well.

The Operations Manager attends an introductory session for new privacy officers run by an external provider and joins a network of Privacy Officers for additional support. They make a plan to provide staff with reminders on privacy issues (by email or during weekly stand-ups) at least once a month and will test staff knowledge with a privacy quiz during Privacy Awareness Week.

As part of the privacy strategy approved by Swiftstart's founders, if the full launch of their platform by the end of the year is successful, then next year the Operations Manager will be provided with funding to develop bespoke training material. They also have a commitment from the founders that they will be supported in further advanced privacy training, including a potential privacy certification.

Small business (non-tech) – Green Gardens

Although Green Gardens is a small business with limited resources to dedicate to privacy training, it recognises that it's something that all staff need to have a basic understanding of. As part of the induction process, new employees are required to complete OPC's free online Privacy ABC module which gives a quick overview of privacy.

Independent contractor – Jo Jones

Since Jo Jones is an independent contractor, it's her responsibility to ensure she has the privacy understanding she needs to protect her clients' personal information. Jo Jones has completed the OPC's free online Privacy 101 module. She also completes the Health 101 module, since she deals with clients' health information, to give her a good understanding of the key concepts and definitions contained in the HIPC. As part of her work with community health service providers, she has access to their respective internal privacy policies and has familiarised herself with them. Jo also receives the regular organisation wide email reminders about relevant privacy issues, from each community health service provider she contracts for.

Government agency – The Ministry

The Ministry has categorised its roles and training requirements for each of them. This means that all new-starters to the Ministry receive short privacy training in the forms of e-learning modules and training from managers, and then bespoke additional training depending on the role's likely interaction with personal information. This training is incorporated into other role-based training so that staff understand that keeping personal information safe and using it appropriately are core parts of doing their job. The Ministry's policies and processes require that new staff must complete training before they can handle personal information. Staff must complete refresher training in line with a training schedule

which records who has completed what training and what is required for each role. The privacy teamwork with the learning and development team to make sure that the training is fit for purpose and appropriate for the role's access and use of personal information.