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.