LR3 - Privacy Guidelines

The Act is primarily concerned with good information handling practices, and is made up of information privacy principles. These principles are summarised in the following guidelines.

Guidelines for collecting, using and storing personal information:

- When we collect information we make the purpose known, and only collect it:
  - for purposes connected with the function of the school, and only when it is necessary to have this information
  - directly from the person concerned, unless it is publicly available from elsewhere
  - in as unobtrusive a manner as possible.
- In general, we collect information directly from the person concerned unless it is publicly available from elsewhere or the person's interests are not prejudiced when we collect the information from elsewhere.
  - We have reasonable safeguards in place to protect information from loss, unauthorised access, use, or disclosure. These safeguards include the use of individual logins for computers, and lockable filing cabinets.
- If collecting information from a child, consideration must be given as to the most appropriate way of gathering that information so that it is collected in a 'fair' way eg in an age-appropriate manner.
- If an individual wants access to information we hold about them, we provide it. Individuals may request correction of this information or, when not corrected, that a record of the request is attached to the information.
- We take reasonable steps to make sure personal information is correct, up to date, relevant and not misleading.
- We only keep information for as long as it is needed, and for the purposes for which it was obtained. When a student moves to a new school and their records are requested, we cull the file and forward the remaining relevant information.
- Information is only used for the purposes for which it was obtained except in certain circumstances (for example, for statistical purposes where the person's identity is not disclosed).
- As a general rule, information about any person is not given to a third party without the person's knowledge, unless:
  - the information is already publicly available
  - it is being passed on in connection with a purpose for which it was obtained, for example, to the student's new school.
  - the right to privacy is over-ridden by other legislation
  - it is necessary for the protection of individual or public health and safety.

For most purposes, the best guide is to use good sense and to treat information about people with great respect.

Date of last review: Term 3, 2021
Date of next review: Term 4, 2023 Signed _____

Parents and the Privacy Act

State and state-integrated schools must observe the Privacy Act, and also the Official Information Act, and the Education Act.

Under the Privacy Act, individuals are entitled to access personal information held about them. There is no age limit to this, children and young people have the same rights as everyone else. This means that parents have no automatic right to access all of the information the school may hold about their child.

Parents and guardians are entitled to access educational information, and are usually able to access other information if they request it, through the provisions of the Official Information Act. This act overrides the Privacy Act in most circumstances. In considering a request from a parent, the school must consider the following:

- Is it information that the parent has a right to, for instance, about their child's academic progress, or is it information the child has a right to keep private?
- Is the parent acting as the child's representative, or acting without the child's consent?
- Is the child of an age or maturity that allows them to decide to give consent or not?
- Is disclosure of the information a breach of the child's confidentiality?
- Is it in the child's best interest?
- Does other legislation affect the decision? For example, the Education and Training Act, 2020 (section 103), requires principals to tell parents about matters which are preventing or slowing a student's progress at school, or harming the student's relationships with teachers or other students.

In practice there are very few occasions when a school would be justified in withholding any information from a parent. One example of such a situation might be a child at school who finally has confidence to confide in a counsellor who is trying to help the child and the child insists that the parents or (perhaps in a situation of abuse), a particular parent, are not to be told the child's information by the counsellor. A counsellor is required to respect and consider the wishes of the child.

When in doubt, seek advice. A good place to start is the Office of the Privacy Commissioner.

Note: in the case of separated parents, each parent is entitled to educational information about their child, for example, school reports. These should be provided unless there is a Court Order preventing it. It is the responsibility of the custodial parent to alert the school of any such Order.

Parents have no automatic right to request corrections of information held about their child. The school, however, is bound by the principles of the Privacy Act and one of them is to endeavour to keep information about a person up-to-date and correct. If a parent points out that information is incorrect, the school should correct it.

Parents are not entitled to information about other parents, or students who are not their own children.

Date of last review: Term 3, 2021
Date of next review: Term 4, 2023 Signed _____

Publishing Student Information

The school sometimes publishes students' photographs and work in the newsletter and/or online, and has an obligation to:

- protect students' privacy and safety in relation to information about them, or images of them, published by the school, and
- protect students' copyright in relation to the material they create.

Images of students and/or their work are published to recognise student achievement, report on learning to the school and wider community, and to promote the school.

The following guidelines help us to protect our students:

- The school seeks parents' written consent before their child's photo or work is published online. Parents give this consent at enrolment, or verbally for social occasions at their discretion. Parents can withdraw their consent at any time.
- The school takes special care with personal information about students, that is, information that identifies an individual. With consent, we share no more than a student's first name and/or photograph via the newsletter, or the wider online community via the school website.
- The school publishes photos and students' work that positively depict the student and school.
- The school seeks students' consent before publishing their work.
- As the author of a copyright work, a student has the right to be identified when their work is exhibited in public, such as on the internet. At Timaru Christian School we prefer to identify the student by their first name and year at school only to protect their privacy. Requests for a child's full name to be published are considered by the privacy officer.

If the school is aware of a special circumstance regarding a student's presence at the school, such as a court order preventing access to the child, any information that could identify the child is kept out of the website/newsletters.

Disclosing information overseas

Personal information may only be disclosed to an overseas agency if that agency has a similar level of protection to New Zealand, or the individual is fully informed and authorises the disclosure.

Note: The following steps are recommended by the Office of the Privacy Commissioner

Responding to privacy breaches

If you become aware of a privacy breach at your organisation, respond as quickly as possible. This will help minimise any harm caused to the affected people and your organisation.

These are four key steps in dealing with a privacy breach:

1. **Contain**
2. **Assess**
3. **Notify**
4. **Prevent**

Date of last review: Term 3, 2021
Date of next review: Term 4, 2023 Signed _____

Complete the first three steps either at the same time or in quick succession.

Every privacy breach has a different level of risk and impact. Evaluate and respond to them on a case-by-case basis.

Step 1: Contain

Once you discover a privacy breach, contain it immediately and find out what went wrong. You could contain a breach by:

- trying to get lost information back
- disabling the breached system
- cancelling or changing computer access codes
- trying to fix any weaknesses in your organisation's physical or electronic security.

Inform the person in your organisation who is responsible for privacy issues and figure out who else you need to tell. Consider whether to inform your:

- insurer
- internal auditors
- risk managers
- legal advisers.

Notify Police if the breach appears to involve theft or other criminal activity.
Be careful not to destroy evidence that your organisation or Police might need to find the cause of the problem or fix the issue.

Step 2: Assess

Assessing the risks of the privacy breach will help you figure out your next steps.
You can take a self-assessment to help you determine the seriousness of your privacy breach using our NotifyUs tool.
You should consider:

The types of personal information involved

The more sensitive the information, the higher the risk of harm to the people affected.
A combination of personal information is usually more sensitive than a single piece of personal information. Health information, driver licence numbers, and credit card details can all cause harm on their own, but together they could be used for identity theft.

What the personal information might show

For example, a list of customers on a newspaper delivery route may not be sensitive. But the same information about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

If the personal information is easy to access

If the information doesn't have a password or encryption, then there's a greater risk of someone misusing it.

The cause of the breach

Try and find out what caused the breach and if there's a risk of further breaches.

The extent of the breach

Try and identify the size of the breach, including:

- how many people can access the lost information
- how many people have lost personal information
- the risk of the information being circulated further
- whether the breach is the result of a systemic problem or an isolated incident.

The potential harm resulting from the breach

Think about this from the point of view of the people affected. Types of harm could include:

- identity theft
- financial loss
- loss of business or employment opportunities
- significant humiliation or loss of dignity.

Who holds the information now

Information in the hands of people with unknown or malicious intentions can be of great risk to the people affected.
The risk will be lower if you know the information went to a trusted person or organisation, and you expect them to return it.

Step 3: Notify

You should be open and transparent with people about how you're handling their personal information.
If a privacy breach creates a risk of harm to someone, you should probably notify them. Notifying them promptly means they can take steps to protect themselves and regain control of their information as soon as possible.
Do not notify people unless you're sure that the breach has compromised their information. Notifying the wrong people by mistake can cause unintentional damage.
Organisations will need inform the office of the Privacy Commisioner of serious privacy breaches from 1 December 2020.
Use our online NotifyUs tool to help you assess and report privacy breaches: NotifyUs of a privacy breach.

When to notify

It isn't always necessary to notify people of a breach. If there's no risk of harm, notifying may do more harm than good.
You need to consider each incident on a case-by-case basis. Think about:

- the risk of harm to people affected
- whether there's a risk of identity theft or fraud
- whether there's there a risk of physical harm
- whether there's a risk of humiliation, loss of dignity, or damage to the person's reputation or relationships. For example; if the lost information includes mental health, medical, or disciplinary records.
- what affected people can do to avoid or minimise possible harm, e.g. change a password
- whether you have any legal or contractual obligations.

Use all the facts you have about the situation to decide whether you should notify the people affected.
If you decide to notify, do it as soon as reasonably possible. However, if law enforcement is involved, check with them first in case you compromise their investigation.

Mandatory privacy breach reporting

The Privacy Act 2020 will make it compulsory to report privacy breaches that have caused serious harm, or are likely to do so.

Under the changes to the Privacy Act 2020, an organisation will have to notify the Privacy Commissioner of a privacy breach, if it poses a risk of serious harm to individuals. If you are unsure as to whether the breach is a serious one, our NotifyUs tool will help you make that assessment. You can also contact our office and discuss the matter with us.

How to notify affected people

It's usually always best to notify the people affected directly, such as

- by phone
- by letter
- by email
- in person.

You should only notify people indirectly (e.g. through website information, posted notices, or the media) if:

- notifying them directly could cause further harm
- it's too expensive to notify them directly
- you don't know how to contact them.

Consider notifying vulnerable people through or with a support person.

It may be appropriate to notify people in more than one way.

Who should notify

The organisation that has a direct relationship with the person affected should be the one to notify them.

For example, if a retailer loses the credit card information, the credit card company would be the best organisation to inform the customer. But if a courier company leaves a parcel on a doorstep and it's stolen, the organisation that sent the parcel should tell the affected person.

What to say

Your breach notifications should contain:

- information about the incident, including when it happened
- a description of the compromised personal information
- what your organisation is doing to control or reduce harm
- what your organisation is doing to help people the breach affects
- what steps people can take to protect themselves
- contact information for enquiries and complaints
- offers of support when necessary, e.g. advice on changing passwords
- whether your organisation has notified the Office of the Privacy Commissioner
- contact information for the Privacy Commissioner.

Notifying third parties

Consider any obligations of confidentiality and decide whether you should inform:

- Police
- insurers
- professional or other regulatory bodies
- credit card companies, financial institutions or credit reporting agencies
- third party contractors or other parties who the breach may affect
- internal business units
- the board and the government minister
- union or other employee representatives.

Coping with media interest

How you respond to media interest in your breach can just as important to your organisation's reputation as the breach itself.

Get a senior team together immediately to coordinate your organisation's media response. Responding to journalists quickly will show that you're treating the incident seriously and not hiding from news coverage.

Consider your messages carefully before you deliver them. Get the tone right.

Accept the blame and apologise if necessary. Demonstrate empathy for those most affected by the breach. Show that the wellbeing of those who may have been harmed is your organisation's highest priority.

Step 4: Prevent

The most effective way to prevent future breaches is to a well-thought-out security plan for all personal information.

In the aftermath of a breach, take the time to investigate the cause of the breach and update your prevention plan. Review procedures so you minimise the collection and retention of personal information.