# Policy: Privacy Act 2020

## Policy Statement

The Jireh Christian School ("the School") Board is committed to ensuring that the School will comply with the provisions of the Privacy Act 2020 in all respects. This policy applies to all employees, Board and committee members, students and volunteers who may be required to collect, access, use or disclose personal information, who may manage projects or systems that impact on personal information management, or who are responsible for making policy decisions about the way the School manages personal information.

The School will only solicit, collect, retain and disclose personal information that the School needs for lawful purposes. The School recognises that the individuals it collects information about hold a reasonable expectation that their personal information will be treated with utmost care and respect.

## Privacy Guidelines

**Privacy Officer**

1. The Principal is the Privacy Officer.
2. The Privacy Officer deals with requests for personal information and, if required, liaises with the Privacy Commissioner in any investigations. Our Privacy Guidelines seek to ensure compliance at all times with the Information Privacy Principles found in the Privacy Act 2020.

**Collection of Information**

1. Where a process or system can operate without the collection of identifying information, an individual will be permitted to do so anonymously.
2. Personal information will only be collected when necessary and for purposes connected to the function of the School.
3. Personal information should be collected from individuals directly, unless the information is publicly available, the person's interests are not prejudiced or the situation requires that the information be collected from a third party (e.g. guardian/parent of a student, transferring School).
4. When personal information is collected from an individual, they will be told the purpose of collection, who will have access to it, whether that information is compulsory or optional and what rights they have to access and correct that information.
5. Collection of personal information will be fair and we will seek not to intrude on the personal affairs of an individual as much as possible.
6. Where a new collection, use or disclosure of personal information is to become a routine part of the School's process, the Privacy Officer is to be notified.

**Access and Correction of Information**

1. Every individual, or their authorised representative, has the right to request access to the personal information that the School holds about them, or to ask for their personal information to be corrected if they think it is wrong.
2. Requests for information about students will be referred to the Principal who will establish authenticity of request and release information where appropriate under the Act.
3. Any information about any staff member (requested by a third party) will be provided in the first instance to the staff member, unless written or verbal authority is given by that staff member that the information may be provided directly to the person who requested it.

**Security and Retention**

1. The School has a responsibility to protect the personal information it handles against loss, misuse, unauthorised access or disclosure, and modification.
2. The School must not retain personal information for longer than the School has a lawful purpose to retain or use it.
3. The School must ensure that any privacy breach identified is reported promptly to the Privacy Officer in compliance with the Privacy Breach Response Plan.

**Use and Disclosure of Information**

1. Personal information must only be used or disclosed for the purposes for which it was obtained unless:
   1.1. the individual is not identified;
   1.2. the individual consents;
   1.3. the source of the information is publicly available;
   1.4. the use or disclosure of the information is necessary for a lawful purpose (with reliance on the Privacy Principles 10 and 11);
2. The School must take reasonable steps to ensure that personal information is accurate and up to date before using or disclosing it, particularly where this use or disclosure could impact on the rights or interests of the person to whom the information relates.
3. Before sharing personal information with a contracted service provider the School must ensure that the service provider is required and able to provide an adequate level of protection of the personal information.
4. The School will not disclose personal information outside New Zealand unless:
   4.1. a parent authorises the disclosure, recognising that the School cannot guarantee security of the information once outside New Zealand; OR
   4.2. the School reasonably believes the country where the information is sent has comparable privacy safeguards to those found under the Privacy Act 2020.

**The Responsibilities of the Privacy Officer**

1. The Privacy Officer is responsible for:
   1.1. supporting all staff members to understand and comply with the Privacy Guidelines including maintaining and developing relevant procedures, standards and guidelines;
   1.2. assisting with the management of personal requests for information, privacy breaches and other privacy issues;
   1.3. managing privacy complaints from individuals
   1.4. reporting on privacy breaches and general privacy compliance to the Board
   1.5. liaising with third parties in respect of privacy matters, including the Privacy Commissioner or other relevant regulators and individuals.

**Privacy Complaints**

Complaints are made on a Complaints Form which can be accessed on the School website or at the School office. Complaints are given to the Principal and if the complaint is about the Principal then the complaint is given to the Board via the Presiding Member.

**Privacy Breach**

In accordance with the Privacy Act 2020, the Privacy Officer will report any notifiable breaches as soon as possible (i.e. a breached that has caused or is likely to cause serious harm to someone) to the Office of the Privacy Commissioner.

Examples of serious harm include:

- Physical harm or intimidation
- Financial fraud including unauthorised credit card transactions or credit fraud
- Family violence
- Psychological, or emotional harm

If a notifiable privacy breach occurs, the School will also notify affected people/employees as soon as possible.

**Privacy Act Principles**

The Privacy Act 2020 has 13 privacy principles that govern how personal information should be collected, handled and used. Below is a short summary of these Principles.

Principle 1

- Organisations can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should not require identifying information if it is not necessary for your purpose.

Principle 2

- Organisations should generally collect personal information directly from the person it is about.
- Because that won't always be possible, you can collect it from other people in certain situations. For instance, if:
  - the person concerned gives you permission
  - collecting it in another way would not prejudice the person's interests
  - collecting the information from the person directly would undermine the purpose of collection
  - you are getting it from a publicly available source.

Principle 3

- When organisations collect personal information, you must take reasonable steps to make sure that the person knows:
  - why it's being collected
  - who will receive it
  - whether giving it is compulsory or voluntary
  - what will happen if they don't give you the information.
- Sometimes there may be good reasons for not letting a person know you are collecting their information – for example, if it would undermine the purpose of the collection, or if it's just not possible to tell them.

Principle 4

- Organisations may only collect personal information in ways that are lawful, fair and not unreasonably intrusive. Take particular care when collecting personal information from children and young people.

Principle 5

- Organisations must make sure that there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information. This includes limits on employee browsing of other people's information.

Principle 6

- People have a right to ask you for access to their personal information. In most cases you have to promptly give them their information. Sometimes you may have good reasons to refuse access. For example, if releasing the information could:
  - endanger someone's safety
  - create a significant likelihood of serious harassment
  - prevent the detection or investigation of a crime
  - breach someone else's privacy.

Principle 7

- A person has a right to ask an organisation or business to correct their information if they think it is wrong. Even if the organisation does not agree that it needs correcting, the organisation must take reasonable steps to attach a statement of correction to the information to show the person's view.

Principle 8

- Before using or disclosing personal information, organisations must take reasonable steps to check it is accurate, complete, relevant, up to date and not misleading.

Principle 9

- Organisations must not keep personal information for longer than is necessary.

Principle 10

- Organisations can generally only use personal information for the purpose they collected it. An organisation may use it in ways that are directly related to the original purpose, or they may use it another way if the person gives you permission, or in other limited circumstances.

Principle 11

- Organisations may only disclose personal information in limited circumstances. For example, if:
  - disclosure is one of the purposes for which you got the information
  - the person concerned authorised the disclosure
  - the information will be used in an anonymous way
  - disclosure is necessary to avoid endangering someone's health or safety
  - disclosure is necessary to avoid a prejudice to the maintenance of the law.

Principle 12

- Organisations can only send personal information to someone overseas if the information will be adequately protected. For example:
  - the receiving person is subject to the New Zealand Privacy Act because they do business in New Zealand
  - the information is going to a place with comparable privacy safeguards to New Zealand
  - the receiving person has agreed to adequately protect the information – through model contract clauses, etc.
- If there aren't adequate protections in place, organisations can only send personal information overseas if the individual concerned gives their express permission, unless the purpose is to uphold or enforce the law or to avoid endangering someone's health or safety.

Principle 13

- A unique identifier is a number or code that identifies a person in your dealings with them, such as an IRD or driver's licence number. An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation. For example, this prevents the Government from giving you one personal number to use in all your dealings with government agencies. However, an organisation can record (and use) a person's unique identifier so that they can communicate with another organisation about the

individual. Organisations must also take reasonable steps to protect unique identifiers from misuse and make sure they verify someone's identity before assigning a unique identifier.

**This Privacy Policy may be updated.**

The School reserves the right to change this Privacy Policy at any time.

## Legislative Compliance

Privacy Act 2020

## Review schedule: Triennially

| **ADOPTED BY BOARD** | |
|---|---|
| Date 12th September 2017 | Chairperson **R Thornton (Acting)** |

| | | |
|---|---|---|
| Reviewed Date | 1st September 2020 | Chairperson **M Causley** |
| Reviewed Date | 26th March 2024 | Presiding Member **A Coombridge** |