

P031 PRIVACY POLICY

PURPOSE

To outline how ISWA protects the privacy of our students, staff and community members in accordance to the requirements of the *Privacy Act 1988* (Cth) and the 13 Australian Privacy Principles (APPS).

OBJECTIVES

To have clear guidelines to ensure information collected in the course of doing business with ISWA is protected and safe from unauthorised and/or unintended uses. The Policy will outline:

- Who we collect information from;
- The types of personal information collected and held by us;
- How this information is collected and held;
- The purposes for which your personal information is collected, held, used and disclosed;
- How you can gain access to your personal information and seek its correction;
- How you may complain or inquire about our collection, handling, use or disclosure of your personal information and how that complaint or inquiry will be handled; and
- Whether we are likely to disclose your personal information to any overseas recipients

It is noted that employee records are not covered by the Australian Privacy Principles where they relate to current or former employment relationships between the school and the employee.

PRINCIPLES OF POLICY

The following describe the types of personal, sensitive and health information that may be collected as classified by *Privacy Act* (Act):

- **Personal information** including names, addresses and other contact details which enable an individual to be reasonably identifiable; this also includes dates of birth; next of kin details; financial information, photographic images and attendance records.
- **Sensitive information** (particularly in relation to student and parent records) have a higher level of privacy protection than other personal information. It currently includes religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional or union memberships, family court orders and criminal records.
- **Health information** (particularly in relation to student and parent records) including medical records, disabilities, immunisation details, individual health care plans,

counselling reports, nutrition and dietary requirement

KEY RULES

How do we collect your personal information?

- Directly from parent / student via forms, email communication
- Indirectly through independent sources available publicly
- From other people i.e. personal references

How do we use personal information?

Examples:

- Providing education, pastoral care, extra-curricular and health services
- Satisfying our legal obligations including our duty of care and child protection obligations
- Keeping parents informed as to school community matters through correspondence, newsletters and magazines
- Marketing, promotional and fundraising activities
- Supporting the activities of the School Board
- Supporting community-based causes and activities, charities and other causes in connection with the School's functions or activities
- Helping us to improve our day to day operations including training our staff; systems development; developing new programs and services; undertaking planning, research and statistical analysis
- School administration including for insurance purposes
- The employment of staff

Wherever possible, ISWA will obtain consent from the individuals to whom the sensitive information relates. Information may also be collected to lessen or prevent a serious threat to life, health or safety, or 'permitted situations' such as locating a missing person or collection of health information to a health service. Your consent is also explicitly requested at the time of enrolment on the Enrolment Application form.

Storage and security of personal information

The security of your personal information is of importance to us and we take all reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure.

Personal information we hold which is no longer needed is destroyed in a secure manner, deleted or de-identified as appropriate.

How do we ensure the quality of your personal information?

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up to date. We maintain and update personal information upon notification or when we become aware through other means that it has changed.

How do you gain access to your personal information we hold?

You may request access to the personal information we hold about you, or request that we change the personal information, by contacting us at the details below.

Responding to data breaches

ISWA is committed to taking appropriate and prompt action if there are reasonable grounds to believe a data breach may have or is suspected to have occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action and/or notifying affected individuals. The reporting obligations under the Notifiable Data Breaches (NDB) scheme of the Privacy Act requires entities to notify individuals and the Commissioner about 'eligible data breaches'. An eligible data breach occurs when the following criteria are met:

- There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- This is likely to result in serious harm to one or more individuals, and
- The organisation or agency has not been able to prevent the likely risk of serious harm with remedial action.

Privacy complaints

If you wish to make a complaint about a breach by us of the Australian Privacy Principles, you may do so by providing your written complaint by email, letter, or by personal delivery to any one of our contact details as noted below.

We will acknowledge your complaint within 5 days, responding to your concerns and explaining how we propose to proceed. We may seek further information from you in order to provide a full and complete response.

Your complaint may also be taken to the Office of the Australian Information Commissioner.

How can you contact us?

You can contact us about this Policy or about your personal information by:

- Emailing governance@iswa.wa.edu.au
- Calling +61 (0)8 9285 1144
- Writing to our Governance Officer at PO Box 366, Floreat, WA6014

You CANNOT contact us anonymously (i.e. without identifying yourself) or by using a pseudonym.

Changes to our privacy and information handling practices

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website www.iswa.wa.edu.au regularly for any changes.

ROLES AND RESPONSIBILITIES

The following are the prescribed roles and responsibilities in the implementation of this Policy:

Designated role	Responsibilities of role	Other information
Policy Owner	Update internal policies and procedures in line with Privacy Act.	
HR Manager Governance Officer	Ensure staff awareness of obligations under the Privacy Act. Monitor ISWA's compliance to administrative procedures	Induction Procedures Regulatory compliance
Registrar	Ensure student sensitive and health information are safeguarded from unauthorised use through system access security rules and by physical means.	

POLICY BREACHES

Failure to comply with this policy may be a breach of an employee's employment conditions and disciplinary action including termination of employment (where appropriate).

RECORDKEEPING

Name of document	File Location	Security Level
Student health alerts and medical contacts	MAZE SEQTA	All Staff Read Access Only
Student health and other sensitive information, including court orders/family history	W: Drive	Restricted to Registrar, Principal, Principal's Executive Assistant, Governance Officer, Administration Officers
Staff information	MAZE HR drive	Restricted

ASSOCIATED POLICIES AND PROCEDURES

- Duty of Care
- Records Management Policy

Policy Category	Business Services and Administration
Date Approved	July 2015
Frequency for review	Every two years unless required earlier
Policy Owner	Business Manager
Amendment History	
Date	Amendment
April 2020 V1.0	Reviewed and updated (notifiable breaches)