Seventh-day Adventist Schools (WA) Ltd. Privacy Policy

Roles, Responsibilities and Processes

1. Rationale

Seventh-day Adventist Schools (WA) Ltd, trading as Adventist Christian Schools Western Australia (ACSWA), is committed to preserving the privacy in accordance with the Australian Privacy Principles contained in the Commonwealth Privacy Act 1988. This Privacy Policy applies to schools conducted by ACSWA and sets out how ACSWA and its schools manages personal information provided to or collected by it.

ACSWA may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to schools' operations and practices and to ensure the policy remains appropriate to the changing school environment.

2. Aims

This policy aims to ensure that private information collected is:

1. Used for the purpose for which it is collected;
2. Stored securely; and that
3. Breaches of data are dealt with in accordance with the Notifiable Data Breaches (NDB) Act 2017 (Cth)

3. Scope

This policy applies to all ACSWA Schools, and pertains to all personal data collected.

4. Responsibility

To the ACSWA Board of Directors.

5. Point of Contact

Director of Education or Principal.

6. Implementation

6.1. What kinds of personal information does a school collect and how does a school collect it?

The type of information schools collect and hold includes (but is not limited to) personal information, including health and other sensitive information, about:

- pupils and parents and/or guardians (Parents) before, during and after the course of a
  - pupil's enrolment at the school [insert the following as relevant, and add any other
  - general kinds of information]
  - name, contact details (including next of kin), date of birth, gender, language
  - background, previous school and religion;
  - parents' education, occupation and language background;
  - medical information (e.g. details of disability and/or allergies, absence notes,
  - medical reports and names of doctors);
  - conduct and complaint records, or other behaviour notes, and school reports;
  - information about referrals to government welfare agencies;
  - counselling reports;
  - health fund details and Medicare number;
  - any court orders;
  - volunteering information; and
  - photos and videos at school events;
- job applicants, staff members, volunteers and contractors, including: [insert the following as relevant, and add any other general kinds of information]
  - name, contact details (including next of kin), date of birth, and religion;
  - information on job application;
  - professional development history;
  - salary and payment information, including superannuation details;
  - medical information (e.g. details of disability and/or allergies, and medical
  - certificates);
  - complaint records and investigation reports;
  - leave details;
  - photos and videos at school events;
  - workplace surveillance information;
  - work emails and private emails (when using work email address) and Internet
  - browsing history; and

- other people who come into contact with the school, including name and contact details and any other information necessary for the particular contact with the school.

Personal Information you provide:
A school will generally collect personal information held about an individual by way of forms filled out by parents or pupils, face-to-face meetings and interviews, emails and telephone calls. On occasions, people other than parents and pupils provide personal information.

Personal Information provided by other people:
In some circumstances a school may be provided with personal information about an individual from a third party, for example a report provided by a medical professional or a reference from another school.

Exception in relation to employee records:
Under the Privacy Act, the Australian Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the school's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the school and employee.

6.2 How will a school use the personal information you provide?

A school will use personal information it collects from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented.

6.2.1. Pupils and Parents:
In relation to personal information of pupils and parents, a school's primary purpose of collection is to enable the school to provide schooling to pupils enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the school. This includes satisfying the needs of parents, the needs of the pupil and the needs of ACSWA and school throughout the whole period the pupil is enrolled at the school.

The purposes for which ACSWA and its schools uses personal information of pupils and parents includes:

- to keep parents informed about matters related to their child's schooling, through
- correspondence, newsletters and magazines;
- day-to-day administration;
- looking after pupils' educational, social, spiritual and medical wellbeing;
- seeking donations and marketing for the school; and
- to satisfy ACSWA and its schools' legal obligations and allow the school to discharge its duty of care.

In some cases where a school requests personal information about a pupil or parent, if the information requested is not obtained, the school may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

6.2.2. Job applicants and contractors:

In relation to personal information of job applicants and contractors, the school's primary purpose of collection is to assess and (if successful) to engage the applicant or contractor, as the case may be.

The purposes for which a school uses personal information of job applicants and contractors include:

- administering the individual's employment or contract, as the case may be;
- for insurance purposes;
- seeking funds and marketing for the school; and
- satisfying the [CEO's / System's] and the school's legal obligations, for example, in relation to child protection legislation.

6.2.3. Volunteers:

A school also obtains personal information about volunteers who assist the school in its functions or conduct associated activities, such as the Home and School Association, to enable the school and the volunteers to work together.

6.2.4. Marketing and fundraising:

Schools treat marketing and seeking donations for the future growth and development of the school as an important part of ensuring that the school continues to be a quality learning environment in which both pupils and staff thrive. Personal information held by a school may be disclosed to an organisation that assists in the school's fundraising, for example, the school's Foundation or alumni organisation [or, on occasions, external fundraising organisations].

Parents, staff, contractors and other members of the wider school community may from time to time receive fundraising information. School publications, such as newsletters and magazines, which include personal information, may be used for marketing purposes.

6.2.5. Exception in relation to related schools:

The Privacy Act allows each school, being legally related to each of the other schools conducted by ACSWA, to share personal (but not sensitive) information with other schools conducted by ACSWA. Schools may then only use this personal information for the purpose for which it was originally collected by ACSWA and its schools. This allows schools to transfer information between them, for example, when a pupil transfers from an ACSWA school to another school conducted by ACSWA.

6.3 Who might a school disclose personal information to and store your information with?

A school may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include to:

- other ACSWA schools and teachers at those schools;
- government departments (including for policy and funding purposes);

- medical practitioners;
- people providing educational, support and health services to the school, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- people providing administrative and financial services to the school;
- recipients of school publications, such as newsletters and magazines;
- pupils' parents or guardians;
- anyone you authorise the school to disclose information to; and
- anyone to whom we are required or authorised to disclose the information by law, including child protection laws.

6.3.1. Sending and storing information overseas:

A school may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, a school will not send personal information about an individual outside Australia without:

1. obtaining the consent of the individual (in some cases this consent will be implied); or
2. otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The school may use online or 'cloud' service providers to store personal information and to provide services to the school that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's servers which may be situated outside Australia.

An example of such a cloud service provider is Google. Google provides the 'Google Apps for Education' (GAFE) including Gmail, and stores and processes limited personal information for this purpose. ACSWA and school personnel and their service providers may have the ability to access, monitor, use or disclose emails, communications (e.g. instant messaging), documents and associated administrative data for the purposes of administering a cloud based service such as GAFE and ensuring its proper use.

Cloud service providers will only be utilised after the school determines that the provider has adequate privacy protocols in place.

6.4 How does a school treat sensitive information?

Sensitive information is defined as information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or practices or criminal record, that is also personal information; health information and biometric information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

6.5 Management and security of personal information

ACSWA and its schools' staff are required to respect the confidentiality of pupils' and parents' personal information and the privacy of individuals. Each school has in place steps to protect the personal information the school holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password access rights to computerised records.

6.6 Access and correction of personal information

Under the Commonwealth Privacy, an individual has the right to seek and obtain access to any personal information which ACSWA or a school holds about them and to advise ACSWA or the school of any perceived inaccuracy.

There are some exceptions to this right set out in the Act. Pupils will generally be able to access and update their personal information through their parents, but older pupils may seek access and correction themselves.

To make a request to access or to update any personal information ACSWA or a school holds about you or your child, please contact the school's Principal by telephone or in writing.

The school may require you to verify your identity and specify what information you require. The school may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the school will advise the likely cost in advance. If the school cannot provide you with access to the requested information, the school will provide a written notice explaining the reasons for refusal.

6.6.1. Consent and rights of access to the personal information of pupils

ACSWA respects every parent's right to make decisions concerning their child's education. Generally, a school will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's parents. The school will treat consent given by parents as consent given on behalf of the pupil, and notice to parents will act as notice given to the pupil.

Parents may seek access to personal information held by the school or ACSWA about them or their child by contacting the school' Principal or school's Administrator by telephone or in writing. However, there may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the school's duty of care to the pupil.

A school may, at its discretion, on the request of a pupil grant that pupil access to information held by the school about them, or allow a pupil to give or withhold consent to the use of their personal information, independently of their parents. This would normally be done only when the maturity of the pupil and/or the pupil's personal circumstances warrant it.

6.7 Enquiries and complaints

If you would like further information about the way ACSWA and its schools manages the personal information it holds, or wish to complain that you believe that ACSWA or a school has breached the Australian Privacy Principles, please contact the school's Principal in writing. ACSWA or the school will investigate any complaint and will notify you of a decision in relation to your complaint as soon as is practicable after it has been made in accordance with the ACSWA Complaints Handling and Appeals Policy, a copy of which is available on the schools' website.

Document Controls

Document Name	Seventh-day Adventist Schools (WA) Ltd Privacy Policy Roles, Responsibilities and Processes
Status	Draft
Version	1
Created	10 July, 2018
Implemented	Ratified by ACSBOD 26 July 2018
Amended	EDCOM Reviewed 12 July 2018
Change Log	
Acknowledgements	National Catholic Education Commission and Independent Schools Council of Australia Compliance Manual, January 2018.

Appendix

Guidelines for Managing Notifiable Data Breaches

1. Definitions

Term	Definition
Data Breach	A data breach concerns the security of personal information and involves the actual unauthorised access or disclosure of personal information, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure. This includes breaches brought about by malicious acts (e.g. hacking, theft), systems failure, and human error.
Eligible Data Breach (EDB)	A data breach is an EDB if it is likely to result in serious harm to an individual or individuals whose information is involved in a data breach.
Notifiable Data Breach (NDB)	The Notifiable Data Breaches Scheme came into effect from 22 February 2018. It sets out obligations to notify affected individuals and the Information Commissioner about data breaches which fall within the definition of an Eligible Data Breach (EDB).
Office of Australian Information Commissioner (OAIC)	To whom a EDB is reportable.
Serious Harm	This involves considering whether a reasonable person in the school's position conclude that the data breach would be likely (more probable than not) to cause serious harm to any of the individuals to whom the information relates.

2. Handling Data Breaches

In the instance of a data breach, staff should notify the Principal, and the Principal should take the following steps:

a) Notify the Director of Education, who in turn will notify the Chairperson of the Board

The Principal in collaboration with the Director of Education is responsible to ensure that Steps (b) to (e) are carried out as follows.

b) Contain the data breach

As soon as a data breach is suspected, immediate steps should be taken to identify the data breach, and if one has occurred, to contain and limit it. This can but is not limited to

stopping unauthorised disclosure, shutting down the system that was breached, retrieving personal information, or changing computer access privileges or addressing security weaknesses.

c) Assess whether the data breach is an EDB

- Consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the school has reasonable grounds to believe this to the be case, then it is an EDB and the school must notify the individuals affected and the Information Commissioner.

- Take remedial action to reduce the likelihood of harm to the individuals affected. The school should continue to take remedial steps to contain the data breach, and include the steps taken when preparing the Notifiable Data Breach Statement for submission to the Information Commissioner.

- Conduct this assessment expeditiously and, where possible, within 30 days. If it cannot be done within 30 days, document why this is the case.

d) Notify the Information Commissioner of an EDB and notify individuals affected by the EDB, and potential exceptions to notification

- Notify the Information Commissioner via either email or the AOIC website (Notifiable Data Breach Statement form available on the AOIC website)
- Notify affected individuals by either:
    - Option 1: Notifying all individuals. *Note that where the individual being notifies is a pupil, it could be appropriate to notify or guardian instead of or as well as the pupil. The age and maturity of the pupil will be an important factor when considering who to notify.*
    - Option 2: Notifying only those individuals at risk of serious harm

  If neither of these options are practicable:
    - Option 3: Publish the statement on the school's website. If this option is necessary, include an apology and explanation for what has been done or be being done about the Data Breach.

e) Review the data breach/EDB

- Review the incident and take action to prevent further data breaches. The actions taken should be documented. Actions may include but is not limited to:
    I. Fully investigate the cause of the data breach
    II. Develop a Prevention Plan
    III. Conduct audits
    IV. Update the Data Breach Response Plan
    V. Consider changes to policies and procedures
    VI. Revise staff training practises
- Consider reporting the incident to other relevant bodies such as:
    - Police or law enforcement
    - Other external third parties (e.g. Australian Tax Office)

- Australian Cyber Security Centre and related agencies
- Professional bodies
- Credit card companies or financial services providers

3. Breach of the NDB Scheme

The NDB Scheme is enforceable as set out in the Privacy Act. As such, consequences apply if schools breach the requirements that include:

- An investigation by the Information Commissioner into the causes of the data breach/EDB and the school's response.
- A determination by the Information Commissioner that the school take specified steps to remedy noncompliance, perform any reasonable act to redress any loss suffered, pay monetary compensation.
- A request that the school provide an enforceable undertaking that it will take, or refrain from taking, specified action. IN the case of serious or repeated noncompliance; or
- An application by the Information Commissioner to court to impose a civil pecuniary penalty of up to $2.1 million per breach.

4. Voluntary Notification

When a data breach is not an EDB under the NDB Scheme, there may be instances where the Principal and Director of Education considers it necessary to voluntarily notify one or some affected individuals and the Information Commissioner of the data breach with a view to:

- Taking reasonable steps to keep personal information it holds secure;
- Managing reputational impact to the school; or
- Complying with duty of care obligations.

5. Additional Resources

This Policy and Appendix has been prepared using information from the following documents:

1. National Catholic Education Commission and Independent Schools Council of Australia

   Compliance Manual, January 2018.

   A copy of this manual is accessible via the members' section of the AISWA website.

   The Compliance Manual is specifically for the Education Sector, and contains useful resources and templates including:

   - Annexure 6 – Mandatory Notification of Eligible Data Breaches Summary (a flowchart for managing an EDB) (page 124)
   - Annexure 7 – Data Breach Risk Assessment Factors (a tool useful for identifying an EDB) (pages 125 – 127)
   - Annexure 8 – Template Data Breach Response Plan (a sample template) (pages 128, 129)

2. Office of Australian Information Commissioner

   Data Breach Preparation and Response: *A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*, February 2018.

   A copy of this guide can be accessed by visiting Office of Australian Information Commissioner website: oaic.gov.au.

   This document contains useful resources for identifying and managing a NDB. See:

   - Table of Contents (pages 4 – 5)
   - Data Breach Preparation and Response (a flowchart) (page 20)