Privacy Policy and Procedures

Section	Operations
Number	6f
Version	7
Page	1 of 26
Approved	ASC Board
Date	December 2022
Review	December 2025

Executive Summary:

The Anglican Schools Commission (ASC) seeks to ensure compliance with the Privacy Act 1988 when using and managing personal and sensitive information, collected about individuals who come into the school community and ASC office including staff, students and contractors.

Key Actions:

- Maintain a register of all notifiable data breaches**.**
- Appoint a Privacy Officer.
- Ensure that the School Privacy Policy shall be publicly available.
- Manage breaches in accordance with the Managing a Data Breach – Procedures.
- Ensure all forms used by the school to collect personal and sensitive information include appropriate collection notices.
- Ensure that all staff shall be appropriately informed in relation to the Privacy Act.
- Ensure that all personal and sensitive information held by the school is properly secured.
- Ensure that the Office of the Australian Information Commissioner (OAIC), Chair of the School Council and the CEO are informed of Notifiable Data breaches.
- Ensuring that the individuals impacted by the data breach are informed.

NB: The list above is not exhaustive, and the policy should be read in full to understand all obligations.

1. PURPOSE

The Anglican Schools Commission (ASC) and its schools have a responsibility to:

- use and manage personal and sensitive information collected by them in accordance with the Privacy Act.
- inform individuals of the purpose of collecting personal and sensitive information.

This policy covers personal information about individuals who come into the school community and ASC office including staff, students and contractors.

2. DEFINITIONS

- *Privacy Act (1988)*

The Privacy Act (1988) includes the Privacy Amendment (Private Sector) Act 2000 and Privacy Amendment (Notifiable Data Breaches) Act 2017.

- *Personal Information*

Personal information is information or an opinion that allows someone to identify the individual that the information or opinion is about. It can range from very detailed information such as medical records to other less obvious types of identifying information such as an email address. Personal information collected about students, parents/guardians (parents), job applicants, staff members, volunteers and contractors includes, but is not limited to name, address and other contact details; date of birth; next of kin details; previous school; medical information; financial information; photographic images; attendance records professional development history; complaint records and investigation reports and leave details.

- *Sensitive Information*

Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, government identifiers, nationality, country of birth, languages spoken at home, family court orders, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, biometric information that is to be used for certain purposes or biometric templates. It also includes health information. 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.

- *Health Information*

Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual has expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service. Health information (particularly in relation to student and parent records) includes medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.

- *Record*

The Privacy Act regulates personal information contained in a 'record'. A 'record' is defined as a 'document' or an 'electronic or other device'. A 'document' includes anything on which there is writing, anything from which sounds, images or writings can be reproduced, drawings or photographs. Some items are excluded from this definition, including a generally available publication (e.g. a telephone directory), and anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

- *Primary Information/Purpose*

When an individual provides, and the ASC or school collects, personal information, the primary purpose of collection will be determined by the context in which the individual gave the information to the ASC or school, for example, to enrol a pupil or to apply for a job. This is the primary purpose of collection even if the organisation has some additional purposes in mind.

- *Secondary Information*

The ASC or school may use or disclose personal information for a secondary purpose if it has the individual's consent. Consent to the use or disclosure can be expressed or implied. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the school. If the ASC or its school's use or disclosure has serious consequences for the individual, the ASC or the school would have to be able to show that the individual could have been expected to understand what was going to happen to information about them and gave their consent. In these circumstances, the ASC or school should seek express consent.

Examples of Secondary Information - Send newsletters, magazines, mail-outs and correspondence.

- *Notifiable Data Breach (NDB) Scheme*

The NDB Scheme requires the ASC and its schools to notify particular individuals and the Office of the Australian Information Commissioner (OAIC) about 'eligible data breaches'.

An eligible data breach arises when the following three criteria are satisfied:

- there is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information that the ASC or its schools holds; and
- this is likely to result in serious harm to one or more individuals to whom the information relates; and
- the ASC or its schools have not been able to prevent the likely risk of serious harm with remedial action.

3. PRINCIPLES

The ASC is firmly committed to and bound by the Australian Privacy Principles (APPs) (Appendix 1) contained in the Commonwealth Privacy Act (1988).

This Privacy Policy applies to the ASC and its schools and sets out how the ASC and each school manages personal information provided to or collected by it.

The ASC may, from time to time, review and update this Privacy Policy to take into account new laws and technology, changes to operational procedures and ensure it remains appropriate to the changing work environment.

3.1 The Collection of Personal Information

The ASC and its schools will collect personal information on individuals for a variety of primary purposes. On occasion, the ASC and its schools will also need to use this same personal information for secondary purposes that less directly relate to the primary purpose for which the information was collected. This will only occur in ways that the individual might reasonably expect or in ways to which consent has been implied or given.

The type of information the ASC and its schools collects and holds includes (but is not limited to) personal information including health and sensitive information, about:

- pupils and parents and/or guardians ('Parents') before, during and after the course of a pupil's enrolment at the school;
- job applicants, staff members, volunteers and contractors, including the ASC Board, school council or committee members, and participants in ASC and school activities, particularly professional development;
- other people who come into contact with the school.

3.1.1 Personal Information provided by the Individual:

The ASC and its schools will generally collect personal information directly from an individual by way of completed forms. However, given the nature of our operations, we also receive personal information by emails, letters, face-to-face meetings and interviews, telephone calls, through financial transactions and through surveillance activities such as the use of CCTV security cameras or email monitoring. Personal information will be provided by parents, pupils, staff members, job applicants, volunteers, contractors, and all others coming into contact with the ASC or schools.

The person collecting the information is expected to ensure that the person supplying the information is aware of the purpose(s) for which the information is being collected.

3.1.2 Personal Information provided by Other People:

In some circumstances the ASC or 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, or a recommendation for Board, council or committee membership.

The person collecting the information is expected to ensure that the person supplying the information is aware of the purpose(s) for which the information is being collected.

3.1.3 Exception in relation to Employee Records:

The Privacy Act does not apply to employee records. As a result, this Privacy Policy does not apply to the ASC's or school's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the ASC or school and employee. Past and present employees of the ASC and its schools cannot automatically access the personal information held about them by the ASC or school.

Where State or Territory health privacy legislation applies, we are still required to protect the privacy of employee health information. This Privacy Policy will apply in those circumstances.

3.2 The Use of Personal Information

Personal information is collected 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 has been provided consent. At the time of collecting personal information, the ASC or school will make it clear to the individual as to the intended uses of the information.

3.2.1 Pupils and Parents:

Collection of personal information of pupils and parents is required for the primary purpose of enabling the school to provide schooling for the pupil. This includes satisfying the needs of parents, the needs of the pupil and the needs of the ASC throughout the whole period the pupil is enrolled at the school.

The purposes for which the ASC and its schools use personal information of pupils and parents include:

- 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 the ASC's and the school's 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.

3.2.2 Job applicants, staff members and contractors:

Personal information held about job applicants, staff members and contractors is collected and held for the primary purpose to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be.

In relation to unsuccessful job applicants, permission will be sought to hold the information for any extended period, otherwise it will be destroyed after a period of no more than 60 days.

The purposes for which personal information of job applicants, staff members and contractors is used include:

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

3.2.3 Volunteers:

Personal information about volunteers who assist the ASC or schools in their functions or conduct associated activities, such as alumni associations, the ASC Board and school council or committee members, is collected to enable the ASC, schools and the volunteers to work together.

The purposes for which personal information of volunteers is used include:

- to keep volunteers informed of matters relating to ASC or school activities of relevance for the volunteer to fulfil their obligation;
- for insurance purposes;

- seeking funds and marketing for the ASC or school;
- to satisfy the ASC's and the school's legal obligations, for example, in relation to child protection legislation.

3.2.4 Marketing and fundraising:

Marketing and seeking donations for the future growth and development is an important part of ensuring that the ASC or school continues to be a quality-learning environment in which both pupils and staff thrive. Personal information held maybe disclosed to an organisation that assists in the fundraising, for example, an Alumni organisation.

Parents, staff, contractors and other members of the wider ASC or school community may from time to time receive fundraising information. Publications, like newsletters and magazines, which include personal information, maybe used for marketing purposes. Sensitive information will not be used for this purpose without the consent of the individual.

3.2.5 Exception in relation to related schools:

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

3.3 The Disclosure of Personal Information

The ASC and its schools only use personal information for the purposes for which it was given, or for purposes which are related (or directly related in the case of sensitive information) to one or more of our functions or activities. At the time of collecting personal information, the ASC and its schools will make it clear to the individual as to the potential disclosures of the information.

An ASC school may disclose personal information, including sensitive information, held about an individual to:

- The ASC office;
- another school;
- government departments;
- the School's local parish;
- medical practitioners;
- people providing services to the school, including specialist visiting teachers, counsellors and sports coaches;
- third party vendors providing educational and administrative services to the School;
- recipients of school publications, like newsletters and magazines;
- parents;
- anyone to whom the school has been authorised by you to disclose the information; and
- anyone to whom we are required to disclose the information by law.

3.3.1 Sending information overseas:

The ASC and its schools may disclose personal information about an individual to overseas recipients, for instance, organising an overseas excursion, facilitating a student exchange, or when storing personal information with 'cloud' service providers situated outside Australia or to facilitate a school exchange.

However, personal information about an individual will not be sent outside Australia unless:

- we obtain the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the APPs or other applicable privacy legislation; or
- we form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
- we are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

The data centres used external to Australia have similar regulatory requirements as that of the Commonwealth Privacy Act. One such example is an email service that sends bulk email to our parents. In this situation, only the parents' names and email addresses are uploaded. No information is provided that is irrelevant.

3.3.2 Disclosure of sensitive information:

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

3.4 The Management and Security of Personal Information

The ASC and school staff and individuals who serve on Boards, councils or committees conducting the business of the ASC and its schools are required to respect the confidentiality of personal information and the privacy of individuals.

The ASC and its schools store personal information in a variety of formats including on databases, in hard copy files and on personal devices including laptop computers, mobile phones, cameras and other recording devices.

The ASC and its schools have procedures in place to protect the personal information it holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including locked storage or paper records and password-protected access rights to computerised records.

The ASC or its schools will only identify information about an individual by their name or, if appropriate, an identifier of its own creation.

3.4.1 The Updating of Personal Information

The ASC and its schools endeavour to ensure that the personal information held is accurate, complete and current. A person may seek to update their personal information by contacting the relevant body at any time.

The APPs require the ASC and its schools not to store personal information longer than necessary.

3.4.2 Notifiable Data Breach

The ASC and its schools are required to notify individuals of specific data breaches that affect them and notify the OAIC. When managing a data breach the ASC and its schools will:

- Determine whether it is an eligible data breach (*Unauthorised access, Unauthorised disclosure and/or Loss of* personal information;
- Determine whether the data breach is likely result in serious harm to an individual whose personal information was part of the data breach;

Once it is determined that an eligible data breach has occurred, the ASC and its schools will:

- Prepare a statement capturing a description of the data breach, the kind/s of information concerned, all recommendations;
- Give a copy of the statement to the OAIC as soon as practicable after the school becomes aware of the data breach;
- Notify individual(s) as soon as practicable; and
- Record the data breach in the School Notifiable Data Breach Register.

3.5 Accessing and Correcting Personal Information

In accordance with the Privacy Act, an individual has the right to obtain access to any personal information which the ASC or school holds about them and to advise the ASC or the school of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Pupils will generally have access to their personal information through their parents, but older pupils (18 and over) may seek access and corrections themselves.

A request to access or update any personal information held by the ASC or school is to be provided in writing to either the Chief Executive Officer (CEO) or the relevant Principal. In processing such requests, the CEO or Principal will be guided by the APPs.

Identity verification and specific details on required information may be requested prior to disclosure. A fee maybe charged to cover the cost of verifying the application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, advice on the likely cost should be provided in advance. If the ASC or school cannot provide you with access to that information, a written notice explaining the reasons for refusal will be provided.

3.6 The Right of Access to Personal Information of Pupils

The ASC and its schools respect every parent's right to make decisions concerning their child's education.

Generally, any request for consent and notices in relation to the personal information of a pupil will be referred to the pupil's parents. Consent given by parents will be treated 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 a school or the ASC about them or their child by contacting the school's Principal. However, there will be occasions when access will be 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 so warranted.

3.7 Enquiries and Complaints

If you would like further information about the way the ASC and its schools implement this policy and manage the personal information they hold, or you believe that the ASC or a school has breached the APPs, you may contact the CEO of the ASC or the relevant school's Principal to register a complaint.

The CEO or relevant school Principal 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.

3.8 Review

The ASC and its schools will review all relevant documentation, including standard collection statements and all other forms, as necessary.

4 PROCEDURES: ROLES AND RESPONSIBILITIES

The Privacy Policy and Procedures set out how the ASC and its schools manage personal information provided to or collected by it. The ASC and its schools are bound by the APPs contained in the Commonwealth Privacy Act.

All staff members have a contractual obligation in terms of confidentiality of school information and are required to abide by the regulations of the Privacy Act as outlined in the ASC's Privacy Policy.

4.1 The Anglican Schools Commission

The Anglican Schools Commission Office will:

- Comply with the APPs **(Appendix 1).**
- Implement good privacy governance to ensure compliance with the APPs **(Appendix 2);**
- Develop a School Privacy Policy **(Appendix 3)**;
- Manage breaches in accordance with the **Managing a Data Breach – Procedures (Appendix 4);**
- Maintaining a register of all notifiable data breaches **(Appendix 5);**
- If necessary, assist the Principal or their delegate when a notifiable data breach has occurred; and
- Provide any other assistance to the Principal or their delegate to ensure other aspects of the Privacy Policy are met.

4.2 The Principal

The Principal is responsible for:

- Complying with the APPs **(Appendix 1)**;
- Implementing good privacy governance to ensure compliance with the APPs **(Appendix 2)**;
- Appointing a Privacy Officer, who is responsible for managing privacy on a day to day basis;

- Ensuring that the School Privacy Policy **(Appendix 3)** shall be publicly available;
- Managing breaches in accordance with the **Managing a Data Breach – Procedures (Appendix 4);**
- Maintaining a register of all notifiable data breaches. **(Appendix 5)**;
- Ensuring all forms used by the school to collect personal and sensitive information shall reflect essential information required for the primary purpose of the school. The appropriate collection notice must be attached to each form. Collection notices are available from the ASC;
- Ensuring that all staff shall be appropriately informed in relation to the Privacy Act 1988;
- Ensuring that all personal and sensitive information held by the school is properly secured;
- Ensuring that school-based staff are entitled to view and access records on their personnel file;
- Ensuring that the OAIC is notified of all notifiable data breaches. The Chair of the School Council and the ASC CEO must also be informed; and
- Ensuring that the individuals impacted by the data breach are informed.

4.3 The OAIC (NDB Scheme)

- Receiving notifications of notifiable data breaches;
- Encouraging compliance with the scheme, including by handling complaints, conducting investigations, and taking other regulatory action in response to instances of non-compliance;
- Offering advice and guidance to regulated organisations and providing information to the community about the operation of the scheme.

APPENDIX 1

Australian Privacy Principles (APPs)

Schedule 1 of the Privacy Act (1988)

APP 1 — Open and transparent management of personal information

Ensures that the ASC and its schools manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires the ASC and its schools give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when the ASC and its schools can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how the ASC and its schools must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances the ASC and its schools that collect personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which the ASC and its schools may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps the ASC and its schools must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

The ASC and its schools must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

The ASC and its schools must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. The ASC and its schools have obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines the ASC and its schools' obligations when individuals request to be given access to personal information held about them by the ASC and its schools. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines the ASC and its schools' obligations in relation to correcting the personal information it holds about individuals.

APPENDIX 2

Example of Good Privacy Governance

The four steps that the OAIC expects organisations to take to ensure good privacy governance and compliance with the Privacy Act are:

STEP 1: EMBED

To embed a culture of privacy, make a commitment to:

- treat personal information as a valuable asset to be respected, managed and protected. Outline how protecting personal information is important;
- appoint key roles and responsibilities for privacy management, including a senior member of staff with overall accountability for privacy. Also have staff responsible for managing privacy, including a key privacy officer, who are responsible for handling internal and external privacy enquiries, complaints, and access and correction requests;
- adopt a *'privacy by design'* approach whereby privacy compliance is considered when dealing with personal information right from the start, rather than being considered afterwards;
- allocate resources to support the development and implementation of a privacy management plan that aligns your business processes with your privacy obligations. Your plan should outline how you will implement and monitor the steps outlined in this Framework, and meet your goals or objectives for managing privacy;
- implement reporting mechanisms that ensure senior management are routinely informed about privacy issues;
- understand your privacy obligations. The *APP guidelines* provide guidance on how the OAIC will interpret the APPs and what matters it may take into account when exercising its functions and powers; and
- understand the role of the OAIC. The *Privacy regulatory action policy* explains the OAIC's approach to using its privacy regulatory powers and how it will communicate information.

STEP 2: ESTABLISH

To establish good privacy practices, procedures and systems, make a commitment to:

- keep information about your business's personal information holdings (including the type of information you hold and where it is held) up to date. This includes information held offshore, or that is in the physical possession of a third party;
- develop and maintain processes to ensure you are handling personal information in accordance with your privacy obligations. Ensure these processes:
    - address the handling of information throughout the information lifecycle — prior to collection, once personal information has been collected, while you hold it and once it is no longer needed. Ensure additional consideration is given to areas you assess as having greater risk, including sensitive information and use of service providers, contractors, outsourcing arrangements and offshore storage;
    - clearly outline how staff are expected to handle personal information in their everyday duties. Tailor these processes to align with the different needs of different parts of your business, and how they use personal information.
- promote privacy awareness within your entity by integrating privacy into your induction and regular staff training programs (including short-term staff, service providers and

contractors). This should include training staff on their privacy obligations and your processes. The OAIC has a number of *training resources* to help you with this;

- develop and implement a clearly expressed and up to date privacy policy. Ensure your privacy notices are also up to date and consistent with your privacy policy. The *Guide to developing an APP privacy policy* provides tips and a checklist to help you develop and assess your privacy policy;
- implement risk management processes that allow you to identify, assess and manage privacy risks across your business, including personal information security risks. The *Guide to securing personal information* provides steps and strategies you should consider taking to protect personal information, including privacy impact assessments, information security risk assessments and regular reviews of your personal information security controls;
- undertake privacy impact assessments for business projects or decisions that involve new or changed personal information handling practices (including implementing new technologies). The *Guide to undertaking privacy impact assessments* includes information on threshold assessments, which will help you determine whether a privacy impact assessment is necessary;
- establish processes for receiving and responding to privacy enquiries and complaints. The *Handling privacy complaints* resource provides information to help you address a privacy complaint;
- establish processes that allow individuals to promptly and easily access and correct their personal information; and
- develop a data breach response plan. The *Data breach notification — A guide to handling personal information security breaches* provides guidance to assist you respond effectively to data breaches.

STEP 3: EVALUATE

To evaluate your privacy practices, procedures and systems, make a commitment to:

- monitor and review your privacy processes regularly. This could include assessing the adequacy and currency of your practices, procedures and systems, including your privacy policy and privacy notices, to ensure they are up to date and being adhered to;
- document your compliance with your privacy obligations, including keeping records on privacy process reviews, breaches and complaints. Ensure senior management and those with responsibility for privacy management are briefed on risks or issues identified;
- measure your performance against your privacy management plan. Regularly review your implementation of this Framework and your progress towards your objectives or goals; and
- create channels for both your staff and customers to provide feedback on your privacy processes, such as a suggestion box and feedback form.

STEP 4: ENHANCE

To enhance your response to privacy issues, make a commitment to:

- use the results of your Step 3 evaluations to make changes to your practices, procedures and systems that improve your privacy processes. Track the performance of any new measures you implement;
- consider having your privacy processes externally assessed to identify areas for improvement;

- consider adopting good privacy practices that go beyond the requirements of the APPs, where appropriate. The *APP guidelines* and other *OAIC resources* provide examples of good privacy practices;
- keep informed of issues and developments in privacy law and changing legal obligations. Subscribe to the OAIC's news email list *OAICnet* for updates and participate in privacy seminars, including the *OAIC's webinars*;
- monitor and address new security risks and threats. Subscribe to *Stay Smart Online Alert Service* and follow the steps it suggests for ensuring online security, including implementing software updates and patches. The *Australian Cyber Security Centre* and *CERT Australia* provide guidance on cyber security issues;
- examine and address the privacy implications, risks and benefits of new technologies. Consider implementing privacy enhancing technologies that allow you to minimise and better manage the personal information you handle;
- introduce initiatives that promote good privacy standards in your business practices. Highlight examples of good personal information handling so that your staff know what is expected of them; and
- participate in Privacy Awareness Week and other privacy events. By bringing privacy into the spotlight, you will ensure your staff remain privacy aware.

Source: OAIC – Privacy management framework: enabling compliance and encouraging good practice

APPENDIX 3

School Privacy Policy

Introduction

This Privacy Policy sets out how [Insert School Name] (the School) manages personal information provided to or collected by it. The School is bound by the Australian Privacy Principles (APPs) contained in the Commonwealth Privacy Act 1988.

The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the School's operations and practices and to make sure it remains appropriate to the changing school environment.

Employee records

Employment records for past and present staff are exempt from the Privacy Act. However, where State or Territory health privacy legislation applies, we are still required to protect the privacy of employee health information. This Privacy Policy will apply in those circumstances.

What is personal information?

Personal information is information or an opinion that allows someone to identify the individual that the information or opinion is about. It can range from very detailed information such as medical records to other less obvious types of identifying information such as an email address. Personal information is collected about students, parents/guardians (parents), job applicants, staff members, volunteers and contractors.

Personal information includes, but is not limited to, name, address and other contact details; date of birth; next of kin details; previous school; medical information; financial information; photographic images; attendance records; professional development history; complaint records and investigation reports and leave details.

Sensitive information includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, government identifiers, nationality, country of birth, languages spoken at home, family court orders, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record.

Health information (particularly in relation to student and parent records) includes medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.

Unsolicited personal information is personal information we receive that we have taken no active steps to collect such as an employment application sent to us by an individual on their own initiative, rather than in response to a job advertisement. We may keep records of unsolicited personal information if the Privacy Act permits it (for example, if the information is reasonably necessary for one or more of our functions or activities). If not, we will destroy or de-identify the information as soon as practicable, provided it is lawful and reasonable to do so.

What kind of personal information do we collect?

We will only collect personal information that is relevant to our relationship with the individual. The type of personal information we collect, and hold includes, sensitive and unsolicited personal information, about:

- students and parents or guardians before, during and after the course of the student's enrolment at the School;

- job applicants, staff members, volunteers and contractors; and
- other people who come into contact with the School.

Why do we collect personal information?

The School uses the personal information provided to it, for the primary purpose of education, and for such other secondary purposes as are related to education and reasonably expected, or to which you have consented. This includes satisfying both the needs of parents and the needs of the student throughout the whole period the student is enrolled at the School.

The primary purpose for which the School uses personal information includes, but is not limited to:

- keeping parents informed about matters related to their child's schooling through correspondence, newsletters and magazines;
- day-to-day administration;
- looking after students' educational, social, emotional and medical well-being;
- satisfying the School's legal obligations and allowing the School to discharge its duty of care;
- performing research and statistical analysis;
- protecting the security of our offices, staff, students, visitors and the property held on our premises;
- recruiting staff and contractors to assess and (if successful) to engage the applicant or contractor, as the case may be;
- seeking donations or marketing the School including direct marketing, campaigns, events and competitions.

We may also collect, hold, use and disclose personal information for other purposes, explained at the time of collection, which are required or authorised by or under law or for which permission has been provided.

Volunteers

Personal information about volunteers who assist the Schools in its functions or conduct associated activities, such as alumni associations, the ASC Board and school council or committee members, is collected to enable the ASC, schools and the volunteers to work together.

Direct marketing and fundraising

We may use your personal information to let you know about our products and services. We may contact you for these purposes in a variety of ways, including by mail, email, SMS or telephone. Sensitive information will not be used for direct marketing or fundraising without your consent.

The School treats marketing and the seeking of 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 students and staff thrive. Personal information held by the School maybe disclosed to an organisation that assists in the School's fundraising.

Where you have consented to receiving marketing communications from us, your consent will remain current until you advise us otherwise. However, you can opt out at any time, by:

- contacting us – either via the contact details provided on the communication received, or via the details at the end of this Policy;
- advising us if you receive a marketing call that you no longer wish to receive these calls; or
- using the unsubscribe facility that we include in our commercial electronic messages.

If we have collected personal information that we use to send you marketing communications from a third party, you can ask us to notify you of our information source and we will provide this unless this is unreasonable or impracticable.

Exception in relation to related schools

The Privacy Act allows the School, being legally related to other ASC schools, to share personal (but not sensitive) information. Other ASC schools may then only use personal information for the purpose for which it was originally collected. This allows ASC schools to transfer information between them, for example, when a pupil transfers from an ASC school to another ASC school.

To whom may we disclose your personal information?

From time to time external organisations will have access to the School's data as part of the maintenance of the School's on-site information systems. These organisations can have incidental access to personal information, but they are contractually bound not to copy or disclose any information stored in our systems and the Commonwealth Privacy Act also binds these Australian organisations.

We may share your personal information with third parties where appropriate for the purposes set out under Why Do We Collect Personal Information including, but not limited to:

- other schools and teachers at those schools;
- government departments;
- the school's local diocese and the parish, other related church agencies/entities, and schools with other Dioceses/other Dioceses;
- the Schools local parish;
- assessment and educational authorities;
- people providing administrative and financial services to the School;
- health professionals;
- third parties providing services to the School, including: visiting teachers, sport and other co-curricular coaches, teachers, counsellors and collection agencies;
- third party vendors providing educational and administrative services to the School;
- recipients of our newsletters and magazines;
- pupils' and 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.

Sending information overseas

We may disclose personal information to parties located overseas in the following situations:

- Parents and guardians of students who live overseas, including host families for students on exchange.
- Promotional material will be posted on the School's official social media accounts. Otherwise, staff members are not permitted to copy any personal information about anyone in the School community to any social media sites.

- The School will use cloud-based services, which require some personal information to be sent to data centres external to Australia. Only organisations that have similar regulatory requirements as that of the Commonwealth Privacy Act are used. One such example is an email service that sends bulk email to our parents. In this situation, only the parents' names and email addresses are uploaded. No information is provided that is irrelevant to the operation.
- Individual staff will also use cloud-based services as part of the day-to-day management or assessment of the students in their care. Examples of such services include Office 365, DropBox and Google Docs.
- As part of the day-to-day management or assessment of the students, individual staff will use School-owned Apple devices that synchronise and backup to Apple's iCloud.

How do we collect personal information?

When we collect personal information about you, we will take reasonable steps to outline why we are collecting the information, whether it will be shared and if it is shared, with whom.

We collect personal information in a number of ways, including but not limited to:

- in person – for example, at information mornings or through the School administration;
- from the School website;
- over the telephone;
- face-to-face meetings;
- through hard copy and electronic correspondence, such as letters and emails;
- on forms, both hard copy and electronic – for example, enrolment applications;
- through security cameras;
- from third parties, including doctors and other health professionals.

In some circumstances, the School may be provided with personal information about an individual from a third party; for example: a report provided by a medical professional, a reference from another school or a photograph from the School-appointed photographer. When provided with unsolicited personal information this information will be kept, either destroyed or de-identified as described under unsolicited personal information.

If you don't provide us with your personal information

We will provide individuals with the option of not identifying themselves, or of using a pseudonym, when dealing with us, if it is lawful and practicable to do so.

In some cases, however, if you do not provide us with your personal information when requested, we may not be able to provide you with the product or service that you are seeking. If the School requests personal information about a student or parent, which parents are unwilling to provide, the School may not be able to enrol or continue the enrolment of a student.

Consent and rights of access to the personal information of students

The School respects every parent's right to make decisions concerning their child's education. Generally, the School will refer any request for consent and notices in relation to the personal information of a student to the student's parents or guardians. The School will treat consent given by parents or guardians as consent given on behalf of the student and notice to parents or guardians will serve as notice given to the student.

Individuals may seek access to personal information held by the School about them or their child by contacting the Privacy Officer. However, there will be occasions when access is denied – i.e. when release of the information would have an unreasonable impact on the privacy of others or when the release may result in a breach of the School's duty of care to the student.

Before releasing information, the School may require you to verify your identity and specify the 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.

The School may, at its discretion, on the request of a student, grant that student access to information held by the School about them, or allow a student to give or withhold consent to the use of their personal information independently of their parents or guardians. This would normally be done only when the student involved has reached 18 years of age, but the School could do so in other circumstances when the maturity of the student and/or the student's personal circumstances so warranted.

How do we manage and make secure personal information?

The School staff are required to respect the confidentiality of students and parents' personal information and the privacy of individuals.

We hold personal information in a number of ways, including in hard copy documents, electronic databases, email contact lists, and in paper files. We take reasonable steps to…

- make sure that the personal information that we collect, use and disclose is accurate, up-to-date and complete and (in the case of use and disclosure) relevant;
- protect the personal information that we hold from misuse, interference and loss and from unauthorised access, modification or disclosure; and
- destroy or permanently de-identify personal information that is no longer needed for any purpose that is permitted by the APPs.

You can help us keep your information up-to-date, by letting us know about any changes to your details, such as your name, address, postal address, email address or telephone number. The APPs require the School not to store personal information longer than is necessary.

Notification of Data Breach

If the school discloses your personal information without your permission and not in accordance with this policy, and such breach is likely to result in serious harm, we will notify you and the Office of the Australian Information Commissioner (OAIC). If there is unauthorised access to our information systems and this breach is likely to result in harm, we will notify you and the OAIC.

This notification will include a description of the breach, the kinds of information concerned and the steps to be taken because of the data breach.

If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

Correction of personal information

Please contact our Privacy Officer (details below) if you would like to access or correct the personal information that we currently hold about you. We may ask you to verify your identity before processing any access or correction requests, to make sure that the personal information we hold is properly protected.

Complaints

If you have a complaint about how we have collected or handled your personal information, please contact our Privacy Officer (details below). Our Privacy Officer will endeavour in the first instance to deal with your complaint and take any steps necessary to resolve the matter in a timely manner.

If you are unhappy with our response, you can refer your complaint to the Office of the Australian Information Commissioner or, in some instances, other regulatory bodies, such as the Australian Communications and Media Authority.

Contact details

Please contact the School if you have any queries about the personal information that the School holds or the way that we handle your personal information.

Postal Address:

Privacy Officer

[Insert School Address]:

[Insert Email]:

[Insert Telephone]:

Additional general information about privacy is available on the website of the Office of the Australian Information Commissioner at www.oaic.gov.au or by calling the OAIC's enquiry line at 1300 363 992.

Changes to our Privacy Policy

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website **[insert website]** regularly for any changes.

This Privacy Policy was last reviewed: **December 2022**

APPENDIX 4

Managing a Data Breach - Procedures

Once it is determined that a data breach has occurred, the following steps must be taken:

STEP 1: Contain the Privacy Breach and do a preliminary assessment

a. Immediately notify the Privacy Officer. This notification should include (if known at this stage) the time and date the suspected Privacy Breach was discovered, the type of personal information involved, the cause and extent of the Privacy Breach, and who may be affected by the Privacy Breach.

b. The Privacy Officer must take any immediately available steps to contain the Privacy Breach (e.g., contact the IT department, if practicable, to shut down relevant systems or remove access to the systems, confirm disclosed information has been destroyed).

c. In containing the Privacy Breach, evidence should be preserved that may be valuable in determining the cause of the Privacy Breach. This is particular relevant if there is a Privacy Breach involving information security.

d. The Privacy Officer must consider if there are any other steps that can be taken immediately to mitigate the harm an individual may suffer from the Privacy Breach.

e. The Privacy Officer must make a preliminary assessment of the risk level of the Privacy Breach. This will involve an analysis of the risks involved. The following table sets out examples of the different risk levels.

Risk Level	Description
High	Large sets of personal information or highly sensitive personal information (such as health information) have been leaked externally.
Medium	Loss of some personal information records and the records do not contain sensitive information. Low Risk Privacy Breach, but there is an indication of a systemic problem in processes or procedures.
Low	A few names and school email addresses accidentally disclosed to trusted third party (e.g. where email accidentally sent to wrong person). Near miss or potential event occurred. No identified loss, misuse or interference of personal information.

f. The Privacy Officer must consider if the affected individuals should be notified immediately to mitigate the risk of serious harm to the individuals.

g. The Privacy Officer must escalate **High Risk** and **Medium Risk** Privacy Breaches to the Principal, Chair of the School Council and ASC CEO.

h. If there could be media or stakeholder attention as a result of the Privacy Breach, it must be escalated to the Principal, Chair of the School Council and ASC CEO.

i. If appropriate, the school should consider developing a communications or media strategy to manage public expectations and media interest.

j. If a Privacy Breach creates a real risk of serious harm to the individual, the affected individuals (and their parents if the affected individuals are students) and the OAIC should be notified. **NB:** If remedial action is successful in making serious harm no longer likely, then notification is not required.

STEP 2: Evaluate the risks associated with the Privacy Breach

a. The Privacy Officer must take any further steps available to contain the Privacy Breach and mitigate harm to affected individuals.

b. The Privacy Officer must evaluate the risks associated with the Privacy Breach by:

- identifying the type of personal information involved in the Privacy Breach;
- identifying the date, time, duration, and location of the Privacy Breach;
- establishing the extent of the Privacy Breach (number of individuals affected);
- establishing who the affected, or possibly affected, individuals are;
- identifying what is the risk of harm to the individual/s and the extent of the likely harm (e.g. what was the nature of the personal information involved);
- establishing what the likely reoccurrence of the Privacy Breach is;
- considering whether the Privacy Breach indicates a systemic problem with practices or procedures;
- assessing the risk of harm to the School and the ASC; and
- establishing the *likely* cause of the Privacy Breach.

c. The Privacy Officer should assess priorities and risks based on what is known.

d. The Privacy Officer does not need to consider a particular matter above if this will cause significant delay in proceeding to **STEP 3**.

e. The Privacy Officer should regularly update the Chair of the School Council, Principal and ASC CEO regarding incident status.

STEP 3: Consider Privacy Breach notifications

a. The ASC and its schools are required to notify individuals of specific data breaches that affect them and notify the OAIC. When managing a data breach, the ASC and its schools need to determine whether it is an eligible data breach:

- Does the breach meet one of the following criteria:
  - Unauthorised access – personal information held by the school is accessed by someone who is not permitted;
  - Unauthorised disclosure – personal information held by the school is disclosed or made visible to others outside of the school;
  - Loss – accidental or inadvertent loss of personal information held by the school.
- Would the data breach likely result in serious harm to an individual whose personal information was part of the data breach? Examples of serious harm may include:
  - Identity theft;
  - Significant financial loss by the individual;
  - Threats to an individual's physical safety;
  - Loss of business or employment opportunities;
  - Humiliation, damage to reputation or relationships;
  - Workplace or social bullying or marginalisation.

Once it is determined that an eligible data breach has occurred, the ASC and its schools will:

b. Prepare a statement in accordance with the Act. The statement will set out:

- The identity and contact details of the school;
- A description of the data breach that the school has reasonable grounds to believe has happened;
- The kind/s of information concerned; and
- The recommendations about the steps that individuals should take in response to the data breach that the entity has reasonable grounds to believe has happened.

c. Give a copy of the statement to the OAIC as soon as practicable after the school becomes aware of the data breach;

d. Notify individual(s) as soon as practicable. There are three options for notifying individuals at risk of serious harm, depending on what is practicable for the school:

- notify each of the individuals to whom the relevant information relates – all individuals whose personal information was part of the data breach; or
- notify only those individuals who are at risk of serious harm from the eligible data breach – particular individual or specific subset of individuals involved in an eligible data breach; or
- publish a copy of the statement on its website and take reasonable steps to make the statement public. This may be the preferred approach where the data breach affects both past and present students.

e. Record the data breach in the Notifiable Breach Register.

STEP 4: Take action to prevent future Privacy Breaches

a. The Privacy Officer must enter details of the Privacy Breach and response taken into a Privacy Breach register. The Privacy Breach register must be reviewed each year to identify any reoccurring Privacy Breaches.

b. The Principal must conduct a post-breach review to assess the effectiveness of the School's response to the Privacy Breach and the effectiveness of the Privacy Breach Response Process.

c. The Privacy Officer must, if necessary, make appropriate changes to policies, procedures and staff training practices, including updating this Privacy Breach Response Protocol.

d. The Privacy Officer must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the Privacy Breach and conduct an audit to ensure the plan is implemented.

APPENDIX 5

EXAMPLE: [School] Notifiable Data Breach Register

Number	Date	Description of Breach	Action take to resolve Breach	Reported to OAIC	Reported to School Council Chair	Reported to ASC CEO	Status
1							
2							
3							
4							
5							

Version Control

Version	Date	Summary of Changes
1	Feb-06	New Policy
2	Feb-15	Applies to the ASC / ASC Schools now 6c has been rescinded
3	Feb-18	Include the Notifiable Data Breaches Scheme requirements which come into effect on 22nd February 2018. Inclusion of Procedures – Roles and Responsibilities. Inclusion of Appendix 1 - 6. General Updates.
4	Apr-19	Expanded on the disclosure of information being sent overseas.
5	Jun-19	Expanded to make reference to biometric data.
6	Aug-19	Schools are using collection agencies and are not developing school specific Policy for their websites
7	Dec-22	Annual Policy Review New Format