Privacy Policy

Policy Number	AS22
Policy Owner	Principal
Revision issue date	October 2020

Purpose

The purpose of this policy is to ensure that in the course of Meriden School's activities, we manage and protect personal information in accordance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles.

Scope

This policy applies to all Meriden School staff, students, parents/guardians, contractors, volunteers and visitors to the School.

Policy

The School is bound by the Australian Privacy Principles contained in the Commonwealth *Privacy Act 1988* ('the Privacy Act'). In relation to health records, the School is also bound by the Health Privacy Principles which are contained in the *Health Records and Information Privacy Act 2002* (NSW) ('Health Records Act').

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.

What kinds of personal information does the School collect and how does the School collect it?

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

- students and parents and/or guardians ('Parents') before, during and after the course of a student's enrolment at the School, including:
  - 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
  - photos and videos at School events.
- job applicants, staff members, volunteers and contractors, including:
  - 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
- 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

The School will generally collect personal information held about an individual by way of forms filled out by Parents or students, face-to-face meetings and interviews, emails, telephone calls or electronic means of communication. On occasion, people other than Parents and students provide personal information.

All School families are asked to ensure the School is provided with current personal information. This is best done using the School's on-line, data-base access facility "Parent Lounge".

Similarly, staff are asked to provide and update personal information annually.

Personal Information provided by other people

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 or a reference from another school.

Exception in relation to employee records

Under the Privacy Act and the Health Records Act, the Australian Privacy Principles and Health 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.

How will the School use the personal information you provide?

The 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 by you, or to which you have consented.

Students and Parents

In relation to personal information of students and Parents, the School's primary purpose of collection is to enable the School to provide schooling to students enrolled at the School, exercise its duty of care, and perform necessary associated administrative activities, which will enable students to take part in all the activities of the School. This includes satisfying the needs of Parents, the needs of the student and the needs of the School throughout the whole period the student is enrolled at the School.

The purposes for which the School uses personal information of students and Parents include:

- to keep Parents informed about matters related to their child's schooling, through correspondence, newsletters, magazines and electronic media;
- day-to-day administration of the School;
- looking after students' educational, social and medical wellbeing;
- seeking donations and marketing for the School; and
- to satisfy the School's legal obligations and allow the School to discharge its duty of care.

In some cases where the School requests personal information about a student or Parent, if the information requested is not provided, the School may not be able to enrol or continue the enrolment of the student or permit the student to take part in a particular activity.

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 the 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 donations and marketing for the School
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Volunteers

The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as our School Community Groups eg, Meriden Foundation, P and F, JSA, Old Girls' Union, to enable the School and the volunteers to work together.

Marketing and fundraising

The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to provide a quality learning environment in which both students and staff thrive. Personal information held by the School may be disclosed to organisations that assist 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, like newsletters and magazines, which include personal information, may be used for marketing purposes.

Who might the School disclose personal information to and store your information with?

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

- other 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 and/or cocurricular coaches, volunteers, and counsellors
- providers of learning and assessment tools and software vendors that provide educational software to the School (that might be installed on student PCs and tablet devices in agreement with the School).
- 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
- students' parents or guardians
- anyone you authorise the School to disclose information to
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

Sending and storing information overseas

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

- obtaining the consent of the individual (in some cases this consent will be implied)
- 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. School personnel and the AIS and its 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 GAFE and ensuring its proper use. Meriden also uses, for example, Microsoft 365 and Rollmarker.

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: 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 and 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 if the use or disclosure of the sensitive information is allowed by law.

Management and security of personal information

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

The 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.

Responding to Data Breaches

In the event that the School becomes aware of, or has reasonable grounds to suspect, an unauthorised access to, or disclosure of, Personal Information held by the School, or the loss of Personal Information where the loss is likely to result in unauthorised access or disclosure of Personal Information, the School will take appropriate, prompt action to investigate the breach and take remedial action in accordance with the School's Data Breach Response Plan (Appendix 1) to:

- Confirm, contain and keep records of the data breach and do a preliminary assessment
- Assess the data breach and evaluate the risks associated with the Data Breach including if serious harm is likely
- Consider notification requirements (the Office of Australian Information Commissioner ('OAIC') and any affected individuals)
- Review the data breach or Eligible Data Breach to prevent future breaches.

The School has a Data Breach Response Team ('DBRT'). The members of the DBRT are:

- Head of Operations
- Director of ICT
- Director of Compliance
- Dean of Inquiry Learning

Access and correction of personal information

Under the Commonwealth Privacy Act and the Health Records Act, an individual has the right to seek and obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy. Students will generally be able to access and update their personal information through their Parents, but older students may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or to update any personal information the School holds about you or your child, please contact the School 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 we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal.

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 requests for consent and notices in relation to the personal information of a student to the student's Parents. The School will treat consent given by Parents as consent given on behalf of the student, and notice to Parents will act as notice given to the student.

Photography by Parents or Students

Apart from concerts, assemblies and special events, approval must be obtained prior to taking any photographs, recordings or videos around the School. At special events, parents are asked to photograph their own children and should never distribute, store or display photographs of others' children, in either electronic or printed form, without their express permission. Similarly School emblems or icons should not be used without the express permission of the Principal.

Notwithstanding, parents need to be mindful that their children may be photographed by other parents or visitors at Meriden School events or events at other Schools or venues.

Students may only take photographs at school with the permission of their Head of School.

Enquiries and complaints

If further information is required about the way the School manages the personal information it holds, or if anyone wishes to complain that they believe that the School has breached the Australian Privacy Principles the School Principal should be contacted by:

- Emailing: enquiries@meriden.nsw.edu.au
- Writing: Meriden School 10-12 Redmyre Rd Strathfield, NSW 2135
- Telephoning (+61 2) 9752 9444

The School will investigate any complaint and will notify the complainant of the making of a decision in relation to the complaint as soon as is practicable after it has been made.

Related Documents

Information Technology, Computer, Telephone and Equipment Code of Use

Social Networking Policy

Staff Code of Conduct

Staff Guidelines for Laptop Use

Appendix 1

Data Breach Response Plan

1. This Data Breach Response Plan sets out the steps to be taken if the School becomes aware of, or has reasonable grounds to suspect, a data breach has occurred.

2. A data breach occurs when Personal Information held by the School is subject to unauthorised access to, or disclosure or the loss where the loss is likely to result in unauthorised access or disclosure.

3. This Plan is intended to enable assist the School to contain, assess and respond to data breaches and to help mitigate potential harm to affected individuals.

4. There is no single method of responding to a data breach. Depending on the breach, not all steps may be necessary. Each breach should be dealt with on a case-by-case basis.

5. An Eligible Data Breach (as defined by the OAIC) must be notified to the individual(s) involved and the Office of the Australian Information Commissioner (OAIC) (see below).

Step 1 **Contain the breach, keep records and make a preliminary assessment** Note: Steps 1-3 should occur simultaneously or in quick succession**.**	☐	Staff member to notify immediately their Head of School and the Head of Operations of any breach or suspected data breach Staff member to take make a note of time and date of the breach, type of personal information involved and the cause and extent of the suspected breach Head of Operations to notify the Director of ICT and the Director of Compliance.
	☐	Take steps to identify and contain the data breach
	☐	Inform the Principal and Heads and provide ongoing updates
	☐	Ensure evidence is preserved that will assist determining the cause of the breach or future remedial action
	☐	The Head of Operations (or other member of the Data Breach Response Team) is to make a preliminary assessment of the risk level of the data breach. **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 Data Breach, but there is an indication of a systemic problem in processes or procedures **Low Risk** 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.
	☐	Where a **High Risk** incident is identified, the Head of Operations must consider (with the assistance of the DBRT) if any of the affected individuals should be notified immediately where serious harm is likely. Any such notification should come from the Principal or a delegated senior staff member.
	☐	The Head of Operations must escalate **High Risk** and **Medium** Risk Data Breaches to the DBRT.
	☐	If there could be media or stakeholder attention as a result of the data breach it must be escalated to the DBRT
	☐	Consider developing a communications or media strategy to manage public expectations and media interest. Contact the Director of Marketing
	☐	The Director of Compliance is to keep records of the breach and action taken including a written report of the breach (see Template below) and to table any report at the next ICT meeting
Step 2 **Evaluate the risks for individuals associated with the breach**	☐	The DBRT is to take any further steps (in addition to above) to **contain** the data breach and mitigate or remediate harm to affected individuals
	☐	The DBRT is to take any further steps (in addition to above) to **contain** the data breach and mitigate or remediate harm to affected individuals * The Director of Compliance is responsible for maintaining any records of the DBRT.
	☐	The DBRT is to **evaluate risks** associated with the data breach, including by: • Identifying the type of personal information involved in the data breach • Identifying the date, time, duration, and location of the data breach • Establishing who could have access to the personal information; • Establishing the number of individuals affected; and • Establishing who the affected, or possible affected, individuals are * The assessment is to be completed asap and in any event within 30 days after knowledge of the data breach
	☐	The DBRT is to **assess whether the data breach is likely to cause serious harm** to any individual whose information is affected by the data breach and is therefore an 'Eligible Data Breach' Serious harm is not defined by the legislation but can take into account: • Risk to individuals' safety • Financial loss to an individual or organisation • Damage to personal reputation or position

		• People having their identities stolen • The private home addresses of protected or vulnerable people being disclosed.
	☐	Report any data breach likely to cause serious harm to the OAIC and affected (see also steps below)
Step 3 **Consider data breach notifications**	☐	The DBRT is to determine whether to notify stakeholders of the data breach even if it is not strictly an eligible data breach. Any such notification should come from the Principal or a delegated senior staff member.
	☐	For any Eligible Data Breach, the DBRT is to prepare a statement for the OAIC (form available on the OAIC website) and give a copy to the OAIC
	☐	For any Eligible Data Breach, the DBRT is to notify affected individuals and inform them of the contents of the statement for the OAIC. The options for notifying are: **Option 1** notify all individuals **Option 2** notify only those individuals at risk of serious harm If neither of these is practicable **Option 3** publish the statement on the School's website and publicise it
Step 4 **Review the incident and take action to prevent future breaches**	☐	The DBRT must conduct a post-breach review to assess the effectiveness of the School's response to the data breach and the effectiveness of the this plan
	☐	The Director of Compliance is to enter details of the data breach and response taken into a Data Breach log to identify reoccurring data breaches (stored in I:drive Compliance)
	☐	The Director of Compliance must, if necessary, make appropriate changes to policies, procedures and staff training practices, including any necessary update to this plan
	☐	The Director of ICT must, if appropriate, develop a prevention plan to address any weaknesses in data handling that contributed to the data breach and conduct an audit to ensure the plan is implemented

Template - Data Breach Report

To be returned by email to the Data Breach Response Team (Head of Operations, Director of ICT, Director of Compliance and Dean of Inquiry Learning) within 3 working days of the breach occurring. The Report is to be tabled at the next ICT meeting.

Report prepared by (Name and role):	
Date of report:	
What were the circumstances of the breach?	*What was the breach?* *When did the breach happened?* *When was the breach discovered? By whom? How was it discovered?* *Who was/were the unauthorised recipient(s) of the personal information?*
What is the type and amount of personal information involved in the breach?	*Who is the information about? e.g. employee, parents, student* *What is the information about the individual? e.g email address, health information, home address, financial information?* *How many people's information was affected? (estimated or actual)*
What remedial action has been taken to contain or control the breach? **Who took the action?**	e.g. changed / revoked passwords, recalled emails
What is the potential harm for the affected individuals?	*For example, could the information be used for identity theft, financial loss, threats to physical safety?*
Who has been notified about the breach?	e.g. Principal, Head of Operations, Director of ICT, Director of Marketing, Director of Compliance
What changes in processes or procedures should be	*What safeguards or measures were in place to prevent a breach of this nature occurring? Why, given these safeguards, did the breach occur?*

considered to prevent or minimise the risk of a reoccurrence?	*What additional or amended measures will be implemented e.g staff training, policy development, improved ICT*
Who at Meriden should people contact concerning the breach?	*Name, title, phone number, email address*: *Is there a separate contact for Media enquiries?*