Privacy Policy

Policy Number	AS22
Policy Owner	Principal
Revision issue date	January 2025
Next Revision date	January 2027

Purpose

The purpose of this policy is to set out how Meriden School ('the School') handles personal information provided to, or collected by, the School and your rights in relation to your information, including how to complain and how we deal with complaints.

This policy should also be read in conjunction with the School's Standard and Employee Privacy Collection Notices published on the School's website.

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').

Under the Privacy Act and the Health Records Act, the Australian Privacy Principles and Health Privacy Principles do not apply to certain treatment of an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record held by the School, where the treatment is directly related to a current or former employment relationship between the School and the employee.

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. The current version of this Privacy Policy is published on our public website.

Kinds of personal information the School collects

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

- students and parents and/or legal 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 spoken at home, previous school and religion
  - parents' education, occupation, marital status, country of birth and language spoken at home
  - health information (e.g. details of disability and/or allergies, dietary requirements, absence notes, immunisation/vaccination details, medical reports and names of doctors)

  - bank account and credit card details
  - results of assignments, tests and examinations
  - 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
  - court orders
  - volunteering information, and
  - photos and videos at School events.
- Employment 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 tax file number, superannuation and bank account details
  - health information (e.g. details of disability and/or allergies, vaccination details and medical certificates)
  - complaint records and investigation reports
  - leave details
  - photos and videos at School events
  - workplace surveillance information, and
  - 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.

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.

How the School collects personal information

Personal Information you provide

The School generally collects personal information held about an individual directly from the individual (or their Parents in the case of students). This includes by way of forms, face-to-face meetings and interviews, emails, telephone calls or electronic means of communication.

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, database access facility "Parent Lounge".

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, a reference from another school or a referee for a job applicant. If a student transfers to a new school, the new school may collect personal information about the student from the student's previous school to facilitate the transfer of the student.

Personal information from other sources

The School may also collect personal information through surveillance activities (such as CCTV security cameras) and email monitoring.

Purposes for which the School collects, uses and discloses personal information

The purposes for which the School collects, uses and discloses personal information depend on our relationship with you and include the following:

Students and Parents

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

- providing schooling and school activities
- satisfying the needs of Parents, the needs of students and the needs of the School throughout the whole period a student is enrolled at the School
- making required reports to government authorities
- keeping Parents informed about matters related to their child's schooling, through correspondence, apps, 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 (see the 'Fundraising' section of this Privacy Policy)
- distribution of surveys for the benefit of 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.

Employment applicants and contractors

- assessing and (if successful) engaging the applicant or contractor
- administering the individual's employment or contract
- for insurance purposes
- seeking donations and marketing for the School (see the 'Marketing and Fundraising' section of this Privacy Policy) (only if a successful applicant)
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Volunteers

- to contact you about, and administer, the volunteer position
- for insurance purposes
- satisfying the School's legal obligations, for example, in relation to child protection legislation

Who the School may disclose personal information to

The School may disclose personal information, including sensitive information, for educational, care and administrative purposes and to seek support and advice. This may include disclosures to:

- the Meriden Old Girls' Union
- other schools and teachers at those schools, including a new school to which a student transfers to facilitate the transfer of the student
- other schools or sporting organisations and their staff for co-curricular activities (e.g. IGSA sport and cadets)
- providers of services for camps, excursions and incursions
- 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
- organisations that assist us with marketing and fundraising (see the 'Marketing and Fundraising' section of this Privacy Policy)
- providers of specialist advisory services and assistance to the School, including in the area of Human Resources, child protection, students with additional needs and for the purpose of administering Google Apps for Education and ensuring its proper use (see further the section below 'Sending and storing information overseas')
- 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)
- agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes
- people providing administrative and financial services to the School
- the third party providers of our information management and storage systems (for the purpose of the providers providing services to the School in connection with the systems
- recipients of School publications, such as newsletters and magazines
- a student's 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 to by law, including child protection laws.

How we store personal information

We store your personal information in hard copy and electronically. We use centralised information management and storage systems provided by third party service providers. Personal information is stored with, and accessible by, the third party service providers for the purpose of providing services to the School in connection with the systems.

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. See further the section below ‘Sending and storing information overseas’.

Sending and storing information overseas

The School may disclose personal information about an individual to overseas recipients in certain circumstances, for instance, to facilitate a school exchange.

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 who 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..

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. Your personal information may be used to make an appeal to you. It may also be disclosed to organisations that assist in the School’s marketing and fundraising activities, for example, the School’s Foundation or alumni organisation and, on occasions, external fundraising organisations.

If you do not want to receive marketing and fundraising communications from us please contact our Director of Marketing on 9752 9444.

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.

These steps include:

- restricting access to information on the School databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities
- ensuring all staff are aware that they are not to reveal or share passwords
- ensuring where personal and health information is stored in hard copy fields that these files are stored in lockable filing cabinets. Access to these records is restricted to staff on a need to know basis

- implementing physical security measures around the School buildings and grounds to prevent break-ins
- implementing ICT security systems, policies and procedures, designed to protect personal information storage on our computer networks, and
- undertaking due diligence with respect to third party service providers who may have access to personal information, including cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

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, and/or correction of, any personal information which a school holds about them. There are some exceptions to this right set out in those Acts.

A student 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.

Parents can log on to the School's Parent Lounge system and correct and update some of their or their child's personal information at any time.

To make a request to access, update or correct any personal information the School holds about you or your child, please contact the School Principal by email, post or telephone (see contact details below). The School may require you to verify your identity and specify what information you require. The School may charge a reasonable fee for giving access to your personal information (but will not charge for the making of the request or to correct your personal information). If the information sought is extensive, the School will advise the likely cost in advance.

If we decide to refuse your request, we will provide you with written notice explaining the reasons for refusal (unless, given the grounds for refusal, it would be unreasonable to provide reasons) and how to complain.

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. Generally, 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.

Parents may seek access to personal information held by the School about them or their child by contacting the Principal by telephone or in writing (see contact details below). However, there may be occasions when access is denied. Such occasions may include (but are not limited to) where the School believes the student has the capacity to consent and the School is not permitted to disclose the information to the Parent without the student's consent, where release of their 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 student.

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. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

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 Head of Student Wellbeing or Head of Junior School.

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:

- **Phase 1:** Confirm, contain and keep records of the Data Breach and do a preliminary assessment.
- **Phase 2:** Assess the Data Breach and evaluate the risks associated with the Data Breach including if serious harm is likely.
- **Phase 3:** Consider notification requirements (the Office of Australian Information Commissioner ('OAIC') and any affected individuals)
- **Phase 4:** Take action 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 STEM (Junior School)

Enquiries and complaints

If you would like further information about the way the School manages the personal information it holds, or wish to complain that you believe that the School has breached the Australian Privacy Principles or the Health Privacy Principles, please contact the School Principal by:

- Emailing: enquiries@meriden.nsw.edu.au
- Writing: Meriden School, 3 Margaret Street, Strathfield, NSW 2135
- Telephoning: (+61 2) 9752 9444

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

If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner (OAIC) via the OAIC website, www.oaic.gov.au.

Related Documents

Information Technology, Computer, Telephone and Equipment Code of Use (AS18)
Social Networking Policy (AS19)

Staff Code of Conduct (AS14)
Staff Guidelines for Laptop Use (AS20)

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 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).

6. The members of the Data Breach Response Team are::

    - Head of Operations
    - Director of ICT
    - Director of Compliance
    - Dean of STEM (Junior School)

Phase1 **Confirm and contain the breach, keep records and make a preliminary assessment** Note: These steps should occur simultaneously or in quick succession**.**	☐	The staff member who becomes aware of the Data Breach or suspects a Data Breach has occurred must: • immediately notify the Head of Junior School or Head of Student Wellbeing and the Head of Operations. • make a note of the time and date of the breach, type of personal information involved and the cause and extent of the suspected breach • take any immediately available steps to identify and contain the Data Breach, and • consider if there are any other steps that can be taken immediately to mitigate or remediate the harm and individual could suffer from the Data Breach. The Head of Operations must notify the Director of ICT and the Director of Compliance.
	☐	Take any further steps to identify and contain the Data Breach.
	☐	The Director of Compliance must inform the Principal and Heads and provide ongoing updates.
	☐	In containing the breach, evidence should be preserved that may be valuable in determining the cause of the breach or future remedial action.

	☐	The Head of Operations (or another 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.
Phase 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 possibly affected, individuals are.
	☐	The DBRT must then **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.
	☐	All reasonable steps must be taken to ensure that the assessment is to be completed as soon as possible and, in any event, within 30 days after knowledge of the Data Breach.
	☐	Report any Data Breach likely to cause serious harm to the OAIC and affected (see also steps below).
Phase 3 **Consider Data Breach notifications**	☐	The DBRT must determine whether to notify relevant stakeholders of the Data Breach (including affected individuals, parents and the OAIC) even if it is not strictly an Eligible Data Breach. Any such notification should come from the Principal or a delegated senior staff member.
	☐	As soon as the DBRT knows that an Eligible Data Breach has occurred or is aware that there are reasonable grounds to believe that there has been an Eligible Data Breach, the DBRT is to prepare a statement with the prescribed information (form available on the OAIC website) and give a copy of the statement to the OAIC.
	☐	After completing the statement, unless it is not practicable, the DBRT must also take such reasonable steps to notify the contents of the statement to affected individuals or those who are at risk from the Eligible Data Breach. 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 to notify some or all of these individuals: **Option 3** publish the statement on the School's website and publicise it and take reasonable steps to otherwise publicise the contents of the statement to those individuals.
Phase 4 **Review the incident and take action to prevent future breaches**	☐	The DBRT must complete any steps in Phase 2 above that were not completed because of the delay this would have caused in proceeding to Phase 3.
	☐	The Director of Compliance must enter details of the Data Breach and response taken into a Data Breach log (stored in I:drive Compliance). The Director of Compliance must, every year, review the Data Breach log to identify reoccurring data 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 Data Breach Response Plan.
	☐	The Director of Compliance must, if necessary, make appropriate changes to policies and procedures and staff training practices, including updating the Data Breach Response Plan.
	☐	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 STEM (Junior School)) 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 happen?* *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 personal 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?*