

Privacy Policy



Date: February 2026
Review: February 2028

1. Introduction

- 1.1 This Privacy Policy (*"Policy"*) outlines how Lauriston Girls' School (*"School"*) uses and manages personal information it receives or collects. Privacy laws regulate how the School can collect, use and disclose personal information. The School is bound by the Australian Privacy Principles (*APPs*) contained in the Commonwealth Privacy Act 1988 (*Cth*).
- 1.2 The School may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to School's operations and practices, and to make sure it remains appropriate to the changing School environment.
- 1.3 The School is also bound by the Health Records Act 2001 (Vic). This legislation contains Health Privacy Principles which are substantially similar to the APPs but are more detailed in dealing with health information. Health information about current and former students and employees is covered by the Health Records Act 2001 (Vic) and the Health Privacy Principles.

2. Application

- 2.1 This Policy applies to all employees, students, parents, volunteers, contractors, visitors and other people who comes in contact with the School. It also applies to service providers and third parties who handle personal information on behalf of the School.

3. Key Roles and Responsibilities for Privacy Management

- 3.1 School Council:
 - Ultimate accountability for privacy governance.
- 3.2 Principal:
 - Responsible for implementing this Policy and fostering a privacy-aware culture.

INSERT POLICY NAME

Privacy Policy



3.3 Privacy Officer:

- Oversees and handles day-to-day privacy-related compliance, enquiries and complaints, and provides Staff guidance.

3.4 Risk & Compliance Manager:

- Supports the Privacy Officer in overseeing and handling day-to-day privacy-related compliance, enquiries and complaints, and provides Staff guidance.

3.5 Information Technology Manager:

- Supports the Privacy Officer in overseeing and handling day-to-day privacy-related compliance, enquiries and complaints, and provides Staff guidance.

4. Definitions

4.1 Personal information includes a broad range of information, or an opinion (true or not), that could identify an individual. It may include names, addresses and other contact details, date of birth, next of kin details, marital status, billing details, financial information, photographic images and attendance records, unique identifiers (such as student numbers or government- issued IDs), and any other information about an identified or reasonably identifiable individual.

4.2 Sensitive Information is personal information that includes information or an opinion about an individual:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- biometric information (including templates and measurements).

INSERT POLICY NAME

Privacy Policy



5. Types of Information

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

- Students and parents and/or guardians before, during and after the course of a student's enrolment at the School;
- Job applicants, employees, volunteers, visitors and contractors;
- Other people who come into contact with the School; and
- Third-party service providers who perform functions on the School's behalf.

6. Personal Information You Provide

6.1 The School will generally collect personal information about an individual by way of forms filled out by parents and / or students, face-to-face meetings and interviews, and telephone calls. On occasions, people other than parents and students provide personal information.

6.2 The School will generally collect personal information directly from the individual unless it is unreasonable or impracticable to do so.

7. Personal Information Provided by Other People

7.1 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.

7.2 Where reasonably practicable, the School will notify the individual about this collection in accordance with APP 5.

8. Exception in Relation to Employee Records

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

8.2 However, health information about employees is regulated by the Health Records Act 2001 (Vic) and this Policy applies to that health information.

INSERT POLICY NAME

Privacy Policy



9. Collection Notices

9.1 The School provides students, parents, contractors, volunteers (*excluding parent volunteer*) and job applicants with a privacy collection notice before personal information is collected and as required basis to communicate:

- the reason for collecting information.
- how the information is used and disclosed.
- how to access, update and correct the information.

9.2 The School may also send out ad hoc collection notices during the year, for example if they are adopting new technologies or processes.

10. Receipt of Unsolicited Information

10.1 The School may receive information about you that they have taken no active steps to collect. If permitted or required by law, Schools may keep records of this information. If not, they will destroy or de-identify the information when practicable, lawful and reasonable to do so.

11. Use of Information

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

The School takes reasonable steps to ensure that individuals are aware of these purposes at the time of collection.

Students and Parents

11.1 In relation to personal information of students and parents, the School's primary purpose of collection is to enable the School to provide ongoing education and pastoral care for students. 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 and beyond.

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

- Keeping parents informed about matters related to their child's Schooling, through correspondence, newsletters and magazines;

INSERT POLICY NAME

Privacy Policy



- Day to day administration;
- Looking after students' educational, social and medical wellbeing;
- Seeking donations and marketing for the School; and
- Satisfying the School's legal obligations and allowing the School to discharge its duty of care.

11.3 The School will not use or disclose sensitive information for direct marketing without consent.

11.4 In some cases where the School requests personal information about a student or parent, if the information requested is not obtained, the School may not be able to enrol or continue the enrolment of the student.

12. Job Applicants, Members of Staff and Contractors

12.1 In relation to personal information of job applicants, Staff and contractors, the School's primary purpose of collection is to assess and (*if successful*) to engage the applicant, Staff or contractor.

12.2 The purposes for which the School uses personal information of job applicants, Staff and contractors include:

- Administering the individual's employment or contract, as the case may be;
- For insurance purposes;
- Seeking funds and marketing for the School; and
- To satisfy the School's legal obligations, for example, in relation to child protection legislation and child safety standards
- Where required by law or contractual obligation, the School may also disclose this information to government agencies, regulatory bodies, and insurers.

13. Volunteers

13.1 The School obtains personal information about volunteers who assist the School in its functions, to enable the School and the volunteers to work together, to satisfy the School's legal obligations, including compliance with child protection legislation and child safe standards.

13.2 The School may also use this information to communicate with volunteers about their role and related activities.

INSERT POLICY NAME

Privacy Policy



14. Marketing and Fundraising

14.1 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 be a quality learning environment in which both students and Staff thrive.

14.2 Personal information held by the School may be disclosed to an organisation that assists in the School's fundraising, for example, the Lauriston Foundation, Lauriston Parents Association, Old Lauristonians Association and School associations.

14.3 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.

If an individual or a parent/guardian does not wish personal information to be disclosed for these purposes, they may contact the Executive Director, Marketing, Admissions and Communications or the Director of Advancement to make the necessary arrangements for the non-disclosure. The School will comply with any such request as required by law.

15. Disclosure of Personal Information

15.1 The School may disclose personal information, including sensitive information, held about an individual to:

- Another School or educational institution, if required by law;
- Government departments, if required by law;
- Medical practitioners;
- People providing services to the School, including specialist visiting teachers and sports coaches;
- Assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA), NAPLAN Test Administration Authorities (*who will disclose it to the entity that manages the online platform for NAPLAN*).
- Recipients of School publications, such as newsletters and magazines;
- Students' parents or guardians;
- Law enforcement agencies;
- Debt collection agencies;
- Government census requirements; and

INSERT POLICY NAME

Privacy Policy



- Anyone the School has been authorised to disclose information to.

15.2 The School takes reasonable steps to ensure that any third party to whom personal information is disclosed complies with the APPs or equivalent protections.

16. Sending Information Overseas

16.1 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*); or
- Otherwise complying with the requirements of APP 8 regarding cross-border disclosure of personal information.

17. Treatment of Sensitive Information

17.1 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, sexual preferences or criminal record, that is also personal information; and health information about an individual.

17.2 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.

17.3 The School will not use sensitive information for direct marketing without consent.

18. Management and Security of Personal Information

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

18.2 The School has in place steps to protect the personal information the School holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and pass-worded access rights to computerised records.

18.3 The School stores all paper and electronic records, including its destruction, in accordance with the School's Record Management Policy.

INSERT POLICY NAME

Privacy Policy



18.4 The School reviews its security measures to maintain best-practice standards.

19. Updating Personal Information:

19.1 The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date.

19.2 A person may seek to update their personal information held by the School by contacting the Receptionist at any time.

19.3 The APPs require the School not to store personal information longer than necessary.

19.4 The School will take reasonable steps to correct personal information if it is satisfied it is inaccurate, out-of-date, incomplete, irrelevant or misleading, or if the individual requests correction.

20. Right to Access Personal Information

20.1 Under the Privacy Act 1988 (Cth), an individual has the right to obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy.

20.2 There are some exceptions to this right set out in the Act. Students will generally have access to their personal information through their parents, but older students may seek access themselves.

20.3 To make a request to access any information the School holds about you or your child, please contact the School's Privacy Officer at Privacy@lauriston.vic.edu.au

20.4 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 request and locating, retrieving, reviewing and copying any material requested.

20.5 If the information sought is extensive, the School will advise the likely cost in advance.

20.6 Requests will be handled in a reasonable time frame, as required by APP 12.4.

21. Consent and Rights of Access to Information Regarding Students

21.1 The School respects every parent's right to make decisions concerning their child's education.

21.2 The School will refer any requests for consent and notices in relation to the personal information of a student to the student's parents.

21.3 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.

21.4 Parents may seek access to personal information held by the School about them or their

INSERT POLICY NAME

Privacy Policy



child by contacting the School's Privacy Officer at Privacy@lauriston.vic.edu.au.

- 21.5** However, there will be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the students.
- 21.6** The School may, at its discretion and 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 so warrant.
- 21.7** The School will consider the capacity of the student to consent on a case-by-case basis, in line with APP Guidelines and the Australian Law Reform Commission recommendations.

22. Medical Information

22.1 Medical information of Staff is covered by the Health Records Act 2001 (Vic) and the Health Privacy Principles. This section of the Policy extends to health information collected by the School about students, Staff as well as students and other individuals and may include:

- Emergency contacts, next of kin;
- Names of doctors, dentists and other health professionals;
- Assessments, referrals, correspondence with parents;
- Health fund details, ambulance subscription and Medicare number;
- Medical background (including conditions, treatments etc.);
- Immunisations;
- Nutrition, dietary requirements; and
- Diagnosis of disorders, learning difficulties.

22.2 Medical information is only collected from individuals, or where the individual is a student, from or with the consent of parents/guardians. This information is collected:

- In order to provide a health service. This includes activities to assess, maintain or improve the individual's health, for diagnosis or treatment or dispensing prescription drugs (as prescribed by a registered practitioner)
- To assess a student's, an employee's, or another individual's ability to participate

INSERT POLICY NAME

Privacy Policy



incertain activities;

- To assess an employee's fitness to return to work after serious illness or injury.

23. Creation and use of online accounts by students under the age of 16 years

23.1 The School recognises that social media and digital platforms present privacy and safety risks for students. The School does not endorse, and strongly discourages, students age 16 and under from creating or using social media accounts, consistent with the minimum age requirements of most social media platforms and the heightened privacy protections for children under Australian law.

23.2 All students 16 years old or below are not allowed to create or keep a social media account.

23.3 The School will take reasonable steps to ensure that any third-party online service provider complies with relevant privacy obligations, including requirements for parental consent where applicable.

24. CCTV and Surveillance

24.1 The School may use CCTV cameras and other surveillance systems on its premises for the purposes of ensuring the safety and security of students, Staff and visitors, and protecting School property.

24.2 Recordings may capture personal information about individuals on School grounds.

24.3 The School will manage these recordings in accordance with the Privacy Act 1988 (Cth), the Surveillance Devices Act 1999 (Vic), and this Policy.

25. Enquiries

25.1 If you would like further information about the way the School manages the personal information it holds, please contact the School's Privacy Officer at Privacy@lauriston.vic.edu.au.

25.2 Any complaints in relation to the School's privacy management will be handled as per the School's Complaints Policy.

25.3 You may also lodge a complaint with the Office of the Australian Information Commissioner (OAIC) if you are not satisfied with the School's response. Contact details for the OAIC are available at www.oaic.gov.au.

INSERT POLICY NAME

26. Privacy Officer

- To ensure effective management of privacy practices, the School has appointed a Privacy Officer. The Privacy Officer is responsible for overseeing our compliance with privacy laws, responding to enquiries and complaints, and promoting a culture of privacy within the School. The Privacy Officer can be contacted at: Email: Privacy@lauriston.vic.edu.au

27. Responding to privacy breaches

- 27.1** Commencing on 22 February 2018, changes to the Privacy Act 1988 (Cth) make it compulsory for Schools to notify specific types of data breaches (*Notifiable Data Breaches NDBs*), to individuals affected by the breach, and to the Office of the Australian Information Commissioner (*OAIC*).
- 27.2** A data breach occurs where “*personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other interference or misuse.*”
- 27.3** As with most of the Privacy Act, this requirement applies to all non-government Schools, unless they have revenue of less than \$3 million and they do not provide a health service.
- 27.4** Not all data breaches will be NDBs. An NDB is defined as a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.
- 27.5** Not all instances of unauthorised access or use of personal information will come under the mandatory reporting regime. The Privacy Act 1988 (Cth) refers to an “*eligible data breach*”, while the OAIC uses the term NDB on their website.
- 27.6** Under the Privacy Act 1988 (Cth), a data breach must be notified where:
- there is unauthorised access to, or unauthorised disclosure of, personal information
 - A reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the personal information relates.

INSERT POLICY NAME

Privacy Policy



OR personal information is lost in circumstances where:

- unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
- assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.
-

Examples of a data breach which may meet the definition of an eligible data breach include when: a device containing a member of the School community's personal information is lost or stolen e.g. a laptop; a database containing personal information is hacked; or personal information is mistakenly provided to the wrong person.

28. Serious Harm

28.1 The Explanatory Memorandum to the Privacy Act 1988 (Cth) explains that serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the School's position would identify as a possible outcome of the data breach.

28.2 The Explanatory Memorandum also emphasises that though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not in itself be sufficient to require notification unless a reasonable person in the School's position would consider that the likely consequences for those individuals would constitute serious harm. It is expected that a likely risk of serious financial, economic or physical harm would be the most common likely forms of "serious harm" that may give rise to the notification.

29. What Happens When There Has Been a Notifiable Data Breach?

29.1 Where an eligible data breach is suspected or believed to have occurred, the School:

- Carries out a risk assessment in the event that an eligible data breach is suspected;
- Prepares a statement of prescribed information regarding an eligible data breach that is believed to have occurred;
- Submits the statement to the OAIC;
- Contacts all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

INSERT POLICY NAME

Privacy Policy



29.2 The steps in managing a Notifiable Data Breach are as follows: -

a) Suspected Eligible Data Breach

- i. If the School suspects an eligible data breach may have occurred, it must conduct a risk assessment which involves:
 - Assessing whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. This must be as prompt and efficient as practicable in the circumstances;
 - Taking all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.
- ii. The School may undertake a risk assessment where an individual has made a complaint in relation to the security of personal information and the School suspects that an eligible data breach may have occurred, but further information is required to ensure the criteria of an eligible data breach is met. If the risk assessment reveals that an eligible data breach has occurred, the School then follows the notification requirements under the Privacy Act 1988 (Cth) and notifies both the OAIC and if practicable, the individual/s affected.

b) Notifying the OAIC

- i. Once a School has reasonable grounds to believe that there has been an eligible data breach, the School:
 - prepares a Statement in the prescribed format
 - gives a copy of the Statement to the OAIC as soon as practicable after the School becomes aware of the eligible data breach.
- ii. The Statement sets out:
 - the identity and contact details of the School;
 - a description of the eligible data breach that the School has reasonable grounds to believe has happened;
 - the kind/s of information concerned;
 - Recommendations about the steps that individuals should take in response to the eligible data breach that the School has reasonable grounds to believe have happened.
- iii. If the School believes that another entity regulated by the Privacy Act 1988 (Cth) is involved in the eligible data breach, the Statement must include information about the other entities.

INSERT POLICY NAME

c) Notifying the Individual/s

- i. As soon as practicable after notifying the OAIC, the School notifies each of the individuals to whom the relevant information relates or notifies each of the individuals who are at risk from the eligible data breach.
- ii. In each case, the School take such steps as are reasonable in the circumstances to notify the individuals. What is practicable will involve considerations about the time, effort or cost of a notification.
- iii. The School will also publish a statement on its website; and take reasonable steps to publicise the contents of the Statement it prepared for the OAIC.

d) Complaints handling and Australian Privacy Principles (APP) breaches

- i. The APPs require the School to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the School's functions or activities that will enable it to deal with enquiries or complaints about its compliance with the APPs.
- ii. The School advises individuals in this Policy of how they may complain about a breach of the APPs and how the School will deal with that complaint.
- iii. A copy of the School's Privacy Policy can be found on the School's website.
Complaints may be made in writing to the School's Privacy Officer at Privacy@lauriston.vic.edu.au, and the School will respond in a reasonable time frame.

30. Consent and young people

(Specific guidance from the Association of Independent Schools)

30.1 The Privacy Act does not distinguish between adults and children and thus clearly envisages that young people are to be afforded rights in respect of their privacy. However, the APPs do not differentiate between children of different ages and thus it is difficult to determine when it is appropriate to seek consent from students.

30.2 In relation to consent and young people, the APP Guidelines provide as follows:

INSERT POLICY NAME

Privacy Policy



The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have Sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise.

An individual aged under 15 is presumed not to have capacity to consent.

- 30.3** The Australian Law Reform Commission (ALRC) also considered the issue of consents by children and young people and recommended that the Privacy Act 1988 (Cth) should be amended to provide that where an assessment of capacity to provide consent '*is not reasonable or practicable*' an individual of the age of 15 or over should be capable of giving consent and a person under that age should be presumed not to be capable of giving consent.
- 30.4** The ALRC also noted that people with parental responsibility had some authority to make decisions on behalf of their children who lacked capacity if it was part of a duty to provide for their welfare but did not suggest that such authority extended to all situations.
- 30.5** In approaching the issue of privacy for Schools it is important to remember that the underlying arrangement between the School and parents is contractual. Parents are engaging the School to provide Schooling for their child on the terms agreed by the parties. The School's authority over the child derives from the contract with the parents and its duties at law.
- 30.6** A parent is recognised by the common law as having the right to make decisions concerning the child's education and to bring up their child in the religion of their choice. In all States and Territories the age of majority is 18 years.

INSERT POLICY NAME

Privacy Policy



30.7 The School will adopt the approach that consent given by parents will generally be treated as consent given on behalf of the student, and notice to parents will act as notice given to the student.

30.8 However, the School will consider the maturity and circumstances of the student and may seek or accept consent directly from students aged 15 and over where appropriate.

31. Relevant Legislations/ Standards

- Privacy Act 1988 (Cth);
- Education and Care Services National Law Act 2010 (Vic);
- Health Records Act 2001 (Vic);
- Children's Services Act 1996 (Vic);
- Children's Services Regulations 2009 (Vic)
- Surveillance Devices Act 1999 (Vic)
- Notifiable Data Breaches scheme (Part IIIC of the Privacy Act 1988 (Cth))

32. Review Date

This Policy will be reviewed every three years with the next review due in January 2029. An interim review may take place following any changes in legislation or in response to any significant changes in operation.

33. Revision History

Version	Date Approved	Approved By	Next Review Date	Notes/Changes Made
1.0	May 2022	Principal	May 2024	Initial issue of Privacy Policy
2.0	25 February 2026	<ul style="list-style-type: none">• Endorsed by Risk Committee• Approved by School Council	31 October 2028	Substantial compliance update: APP terminology, NDB scheme etc.

INSERT POLICY NAME

Privacy Policy



APPENDIX 1: STAFF CHECKLIST – RESPONDING TO A DATA BREACH

This checklist must be followed immediately if you suspect or become aware of a loss, unauthorised access, disclosure, or misuse of personal or sensitive information.

Immediate Actions (All Staff)

- Stop and contain the breach if safe to do so (e.g. disconnect device, recover documents, stop sharing).
- Do not delete or alter any evidence related to the incident.
- Immediately report the incident to the Privacy Officer or your Manager.
- Record what happened, when it happened, and what information may be affected.

Tailored Guidance for Different Staff Groups

For Teachers

- Immediately report lost devices, emails sent to the wrong recipient, or student information shared incorrectly.
- Do not attempt to fix or hide the issue yourself.
- Preserve evidence such as emails, screenshots, or device details.
- Escalate concerns involving student records, wellbeing, medical, or learning data immediately.

For Corporate / Administrative Staff

- Report incidents involving payroll, financial, HR, donor, or parent records immediately.
- Cease processing affected data until advised by the Privacy Officer.
- Assist with accurate incident documentation and timelines.
- Support containment and remediation actions as directed.

Escalation and Assessment (Privacy Officer / Leadership)

- Confirm the nature and scope of the data breach.
- Identify the type of information involved (personal, sensitive, health).
- Assess whether unauthorised access, disclosure, or loss has occurred.
- Determine whether the breach is likely to result in serious harm.
- Complete a risk assessment as soon as practicable and within 30 days if required.

Notification Obligations (If Eligible Data Breach)

- Prepare a Notifiable Data Breach (NDB) statement.
- Notify the Office of the Australian Information Commissioner (OAIC) as soon as practicable.
- Notify affected individuals directly, or indirectly if direct contact is not practicable.

INSERT POLICY NAME

Privacy Policy



- Include recommendations to individuals on steps they should take to protect themselves.
- Publish a notice on the School website if required.

Post-Incident Actions

- Implement remediation and corrective actions to prevent recurrence.
- Review and update policies, procedures, or security controls if required.
- Document the incident, response actions, and outcomes.
- Manage any complaints in accordance with the Complaints Policy.

Key Contact Details

1. Internal Contacts

Privacy Officer – Email: Privacy@lauriston.vic.edu.au

Principal / Risk & Compliance Manager – via School administration

2. External Agency

Office of the Australian Information Commissioner (OAIC) – Notifiable Data Breaches

Website: <https://www.oaic.gov.au/privacy/notifiable-data-breaches>

Online NDB Form: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach>

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

INSERT POLICY NAME

Privacy Policy



APPENDIX 2: DATA BREACH RESPONSE – RACI AND DECISION SUPPORT

RACI Table – Data Breach Response

R (Responsible) – who does the work

A (Accountable) – who owns the decision

C (Consulted) – who provides input

I (Informed) – who is kept aware

Activity	Staff (Teachers)	Staff (Corporate)	Privacy Officer	Principal	School Council
Identify suspected data breach	R	R	A	I	I
Immediate containment actions	R	R	A	I	I
Initial incident recording	R	R	A	I	I
Assess type and scope of data	I	I	R	A	I
Assess likelihood of serious harm	I	I	R	A	I
Determine if eligible data breach	I	I	R	A	I
Notify OAIC	I	I	R	A	I
Notify affected individuals	I	I	R	A	I
Approve public communications	I	I	C	R	I
Post-incident remediation	C	C	R	A	I
Oversight of privacy governance	I	I	C	C	R

INSERT POLICY NAME

Privacy Policy



Decision Flowchart – Is this an Eligible Data Breach?

START

|

Has personal or sensitive information been lost, accessed or disclosed without authorisation?

|-- NO --> Not an eligible data breach → Record incident and close

|-- YES

|

Is unauthorised access or disclosure likely to occur (if information was lost)?

|-- NO --> Not an eligible data breach → Monitor and document

|-- YES

|

Would a reasonable person conclude the breach is likely to result in serious harm?

|-- NO --> Not an eligible data breach → Mitigate and document

|-- YES

|

ELIGIBLE DATA BREACH

→ Notify OAIC as soon as practicable

→ Notify affected individuals

→ Implement remediation and review controls

INSERT POLICY NAME

APPENDIX 3: SUMMARY OF POLICY ACTIONS

- Comply with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth) and Health Privacy Principles under the Health Records Act 2001 (Vic).
- Review and update the Privacy Policy to reflect legislative, technological, and operational changes.
- Ensure School Council maintains ultimate accountability for privacy governance.
- Ensure the Principal implements the Policy and promotes a privacy-aware culture.
- Appoint and support a Privacy Officer to manage privacy compliance, enquiries, and complaints.
- Provide privacy collection notices before or at the time of collecting personal information.
- Collect personal information directly from individuals where reasonable and practicable.
- Notify individuals when personal information is collected from third parties, where practicable.
- Limit use and disclosure of personal information to primary purposes or related secondary purposes, unless consent is obtained or required by law.
- Do not use or disclose sensitive information for direct marketing without consent.
- Implement safeguards to protect personal information from misuse, loss, or unauthorised access.
- Store and destroy records in accordance with the Record Management Policy.
- Ensure personal information is accurate, up to date, and corrected upon request.
- Provide individuals with access to their personal information in accordance with APP 12.
- Manage and assess privacy complaints in line with the Complaints Policy.
- Restrict overseas disclosure of personal information unless APP 8 requirements are met.
- Manage CCTV and surveillance data in accordance with privacy and surveillance legislation.
- Ensure third-party service providers comply with privacy obligations.
- Assess, respond to, and notify eligible data breaches under the Notifiable Data Breaches scheme.
- Conduct a privacy policy review every three years or sooner if required by legislative or operational change.

INSERT POLICY NAME