POLICIES AND PROCEDURES

Privacy Policy

Lauriston GIRLS' SCHOOL

Date **May 2024**

Review **May 2026**

Introduction

This 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.

This policy outlines our commitment and responsibility in managing personal and health information in accordance with the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth), the Privacy and Data Protection Act 2014 (Vic), and the Health Records Act 2001 (Vic).

The Health Records Act 2001 (Vic) contains Health Privacy Principles which are substantially similar to the Australian Privacy Principles but are more detailed in dealing with health information. Health information about current and former employees is covered by the Health Records Act and the Health Privacy Principles.

The School may, from time to time, review and update this 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.

Application

This policy applies to all employees, students, parents, volunteers, contractors, visitors and other people who may come in contact with the School.

Definitions

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.

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

- 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
- some aspects of biometric information

Health Information is information or an opinion about the health, including illness, disability or genetic makeup, of an individual, the provision of health services to an individual, or collected as part of the provision of a health service.

Types of Information

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; and
- Other people who come into contact with the School.

Personal Information You Provide

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.

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 1988 (Cth) 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.

Collection of Personal Information

The School collects personal information necessary for educational, administrative, and support purposes. This may include, but is not limited to, names, addresses, contact details, dates of birth, medical records, and academic progress.

Use of Personal 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 including educational administration, health and welfare, school communications, and legal compliance.

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 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.

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;
- 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.

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.

Job Applicants, Members of Staff and Contractors

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

The purposes for which the School uses personal information of job applicants, staff members 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

Volunteers

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.

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 be a quality learning environment in which both students and staff thrive. Personal information which is not sensitive 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.

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 Director of Marketing and Communications or the Director of Advancement to make the necessary arrangements for the non-disclosure.

Disclosure of Personal Information

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;
- Law enforcement agencies;
- Debt collection agencies; and
- Anyone the School has been authorised to disclose information to.

Sending Information Overseas

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 Australian Privacy Principles.

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

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

Management and Security of Personal Information

The School's staff members 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, 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.

Updating Personal Information:

The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by the School by contacting the

Receptionist at any time. The Australian Privacy Principles require the School not to store personal information longer than necessary.

Right to Access Personal Information

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. 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.

To make a request to access any information the School holds about you or your child, please contact the Principal 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 request and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Consent and Rights of Access to Information Regarding 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.

Parents may seek access to personal information held by the School about them or their child by contacting the Principal. 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 student.

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.

Medical Information

Medical information of Lauriston staff is covered by the Health Records Act and the Health Privacy Principles. This section of the policy extends to health information collected by the School about 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.

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 in certain activities;
- To assess an employee's fitness to return to work after serious illness of injury.

Generation and use of online accounts by students under the age of 13 years

From time to time students will access School approved sites that are relevant to teaching and learning. The School will create online accounts using their Lauriston Girls' School email account. The students will adhere to the Terms and Conditions of the sites.

Enquiries

If you would like further information about the way the School manages the personal information it holds, please contact the Principal's Executive Assistant.

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

Responding to privacy breaches

Commencing on 22 February 2018, changes to the federal Privacy Act 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). A data breach occurs where "personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse interference."

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.

Not all data breaches will be NDBs. A 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. Not all instances of unauthorised access or use of personal information will come under the mandatory reporting regime. The Privacy Act refers to an "eligible data breach", while the OAIC uses the term NDB on their website.

Under the Act 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.

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.

Serious Harm
The Explanatory Memorandum to the Act 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. 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.

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

Each of these steps is explained in more detail below.

Suspected Eligible Data Breach

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.

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 Act and notifies both the OAIC and if practicable, the individual/s affected.

Notifying the OAIC
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.

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.

If the school believes that another entity regulated by the Act is involved in the eligible data breach, the Statement must include information about the other entities.

Notifying the Individual/s
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. 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. 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.

Complaints handling and Australian Privacy Principles (APP) breaches
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.

The School advises individuals in our Privacy Policy of how they may complain about a breach of the APPs and how the School will deal with that complaint. A copy of the School's Privacy Policy can be found on the school's website.

Consent and young people

(Specific guidance from the Association of Independent Schools)

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.

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

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.

The Australian Law Reform Commission (ALRC) also considered the issue of consents by children and young people and recommended that the Privacy Act 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.

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.

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.

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.
For these reasons, one approach would be for the School to adopt the view that in many circumstances, the contract with the parents will govern their relationship with the child in relation to privacy, and thus consents given by parents will act as consents given on behalf of the child and notice to parents will act as a notice given to the child.

However, this approach will not be appropriate in all circumstances. A School should recognise that young people do have rights under the Privacy Act and in some circumstances it would be appropriate to seek consents from them, particularly when they are aged 15 or over, as indicated by the APP Guidelines and ALRC. No doubt in most cases decisions whether to seek information or consents from students or from parents is likely to follow current practices. Thus, for example, where a student puts his or her name down to take part in a team, the student would usually be impliedly consenting to it being disclosed to a relevant party to enable him or her to compete. As a student reaches greater maturity, the more important it will become to consider whether a parent should be asked for consent or the student. Hopefully in most cases common sense will provide the answer.

For example, in most cases it would be appropriate for the School to collect from a mature student personal (and sensitive) information about the student gained through an interview with the student. Also, there will be many instances throughout a student's schooling where it would be impracticable and inappropriate to first obtain a parent's consent when collecting personal information from a student (eg. during day to day classroom activities). In respect of collecting personal information about students from parents, it is suggested that it is sufficient if parents are given a collection notice informing them of the requirements set out in APP 5.2, then students do not have to be specifically informed.

Another potential concern is that students may attempt to claim a right to prevent disclosure of personal information to a parent, such as their School report. The 'standard collection notice' seeks to overcome this by informing parents that the School will disclose personal information about a student to the student's parents. If a student attempted to restrict disclosure of personal information (such as a School report) to a parent, it is reasonably clear that this would be a permitted purpose as being a related purpose to the purpose for which the information was collected. This does not prevent the School exercising its discretion to restrict disclosure of the personal information.

Particular issues may arise in the context of information provided to staff members, including counsellors, by students 'in confidence' that is, where the student has asked or expected the staff member not to disclose it. One factor when considering how to deal with such situations will be the age and capacity of the students to provide or refuse consent.

Legislation

- Privacy Act 1988 (Cth);
- Education and Care Services National Law Act 2010 (Vic);
- Privacy and Data Protection Act 2014 (Vic);
- Health Records Act 2001 (Vic);
- Children's Services Act 1996 (Vic);
- Children's Services Regulations 2009 (Vic)
- Surveillance Devices Act 1999 (Vic)