PRIVACY POLICY

Revised: March 2002, Apr 2014, June 2018
Current Version: June 2018
Review Date: Annually

LAUNCESTON CHRISTIAN SCHOOL

Privacy Policy

Your privacy is important
This statement outlines the Schools' policy on how the School uses and manages personal information provided to or collected by it.

The policy follows the Australian Privacy Principles (APP) contained in the Commonwealth Privacy Act 1988.

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

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

- students and parents and/or guardians ('Parents') before, during and after the course of a student's enrolment at the School;
- job applicants, staff members, volunteers and contractors; and
- other people who come into contact with the School.

The personal information may include educational and academic records, student behaviour and disciplinary records, addresses, dates of birth, phone numbers, health information, physical characteristics, sports information, information about co-curricular activities, church affiliation and family heritage.

Personal Information you provide:
The School will generally collect personal information held about an individual by way of forms filled out by Parents or students, face-to-face meetings and interviews, 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:
The APP do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the School and employee.

How will the School use the personal information you provide?

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

Students and Parents:
In relation to personal information of students and Parents, the School's primary purpose of collection is to enable the School to provide schooling for the student. This includes satisfying both the needs of Parents and the needs of the student throughout the whole period the student is enrolled at the School.

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

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

You may choose to remain anonymous, or to use a pseudonym when dealing with the School where it is lawful and practical to do so. 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, staff members 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:

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

Volunteers:
The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, such as the Parents and Friends, to enable the School and the volunteers to work together.

Marketing and fundraising:
The School treats marketing and seeking donations for the future growth and development of the School as an important part of ensuring that the School continues to be a quality learning environment in which both students and staff thrive. Personal information held by the School

may be disclosed to an organisation that assists in the School's fundraising, for example, the LCS Parents and Friends Association, the LCS Foundation or alumni organisation.

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. A person may opt out of receiving marketing and fundraising material at any time by contacting the School Office on (03)63272854 or by email to office@lcs.tas.edu.au.

Who might the School disclose personal information to?

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

- another school;
- government departments;
- medical practitioners;
- people providing services to the School, including specialist visiting teachers and sports coaches;
- recipients of School publications, like newsletters and magazines;
- Parents; and
- anyone you authorise the School to disclose information to.

Sending information overseas: The School may disclose personal information about an individual to overseas recipients, for instance, when storing personal information with 'cloud' service providers that are situated outside Australia or to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

• obtaining consent of the individual (in some cases, consent will be implied);

or

• otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

How does the School treat sensitive information?

In referring to 'sensitive information', the School means: information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, 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 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.

The School has adopted the Notifiable Data Breach Response Plan (Appendix A) provided by the Office of the Australian Information Commissioner to contain, assess, notify and review any data breach likely to result in serious harm to any individuals whose personal information is involved in the breach.

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 School Office at any time.

The School does not store personal information any longer than is necessary for its primary purpose.

You have the right to check what personal information the School holds about you

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. 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 School Business Manager in writing.

The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

Consent and rights of access to the personal information of students

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

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

Parents may seek access to personal information held by the School about them or their child by contacting the School 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, may result in a breach of the School's duty of care to the student, pose a serious threat, is unlawful, would prejudice negotiations with the individual, contravene a court order, relate to law enforcement or is commercially sensitive. If a request to access personal information is denied, written reasons will normally be given.

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 so warranted.

Enquiries & 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 the School has breached the Australian Privacy Principles, please contact the Business Manager in writing. The School will investigate any complaint and will notify you of the decision in relation to your complaint as soon as practicable. A complaint must be in writing. If there is no response to a complaint from the school after thirty days, a complaint can be made to the Australian Information Commissioner at http://www.oaic.gov.au/privacy/privacy-complaints

The Business Manager can be contacted at: smithg@lcs.tas.edu.au

By Mail: The Business Manager
Launceston Christian School
PO Box 32
RIVERSIDE TAS 7258
Telephone: 03 63272854

Changes to this policy

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

On 22 February 2018 new legislation was enacted regarding the Mandatory Reporting for Notifiable Data breaches. This requires the School to take additional steps to protect data and advise the Commissioner in the event of a data loss or breach that could result in serious harm to any of the individuals whose information was involved. This is deemed to be a “notifiable data breach”.

This document incorporates those changes.

APPENDIX A

Notifiable Data Breach Response Plan

A data breach can take many forms and have many causes. Depending on the circumstances, the extent of interference with personal information will vary, as will the harm suffered by the individuals affected by the interference. Our notification obligations can also vary.

Suspected or known data breach

A data breach occurs when personal information held by the School is misused, interfered with, lost or subject to unauthorised access, modification or disclosure.

1. Contain

The first step is to **contain** a suspected or known breach, where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

2. Assess

The School needs to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If there are reasonable grounds to believe this is the case, then the School must notify.

If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, the School should consider whether **remedial action** is possible. The School will conduct an assessment in three stages:

1. **Initiate:** plan the assessment and form a DBRT
2. **Investigate:** gather relevant information about the incident to determine what has occurred
3. **Evaluate:** make an evidence-based decision about whether serious harm is likely. This decision should be documented.

The School must conduct this assessment within 30 days.

Take remedial action

Where possible, the School should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed, or changing access controls on compromised databases.

If remedial action is successful in making serious harm no longer likely, then notification is not required. Progress to Step 4: Review.

NO — **Is serious harm still likely?** — **YES**

3. Notify

Where **serious harm is likely**, the School must prepare a statement for the OAIC to be submitted as soon as practicable that contains:

- the School's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

The School must also notify affected individuals, and inform them of the contents of this statement.

The School has three options for notifying:

1. Notify all individuals
2. Notify all individuals at risk of serious harm.

OR if 1 or 2 aren't practicable:

3. Publish the statement on the School's public website and publicise it.

The School may provide further information in its notification, such as an apology and an explanation of what they are doing about the breach.

4. Review

Review the incident and take action to prevent future breaches. This may include:

- fully investigating the cause of the breach
- developing a prevention plan
- conducting audits to ensure the plan is implemented
- updating security/response plans
- considering changes to School policies and procedures
- revising staff training practices
- consider a report to the School Board on outcomes and recommendations following the review

The School should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC
- professional bodies
- other entity/ies that may be involved in the breach