VICTORY
Lutheran College

Privacy Policy

EXCELLENCE IN LEARNING | PROMOTE WELLBEING | STRENGTHENING OUR LUTHERAN IDENTITY | BUILDING COMMUNITY | ASSURE OUR FUTURE

1. INTRODUCTION

Victory Lutheran College (the College) is committed to protecting the privacy of individuals and managing personal and health information in an open, transparent, and responsible manner.

All personal information collected, held and stored by the College will be managed in accordance with:

a) Privacy Act 1988 (Cth) including the Australian Privacy Principles (APPs).

b) Health Records Act 2001 (Vic)

c) The Notifiable Data Breaches Scheme (NDB) Scheme

The APPs provide guidelines for how personal information and can be obtained, securely managed and disclosed.

2. PURPOSE

This Policy outlines how the College collects, uses, stores, and discloses personal information in accordance with applicable privacy laws.

This Policy is accessible on the College website.

3. SCOPE

This Policy applies to all personal and health information collected by the College about students, parents/carers, staff, volunteers, contractors, visitors, and community members, in both physical and digital environments.

Employee records are generally exempt from the Australian Privacy Principles where the information relates directly to a current or former employment relationship. Employee records are managed in accordance with workplace legislation and, where applicable, the Health Records Act 2001 (Vic).

4. DEFINITIONS

Term	Definition
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether recorded in a material form or not. This may include a person's name, address, date of birth, contact details, health information, and educational records. Personal and sensitive information handled by the College is regulated primarily under the Privacy Act 1988 (Cth), including the APPs
Sensitive Information	A subset of personal information that is given a higher level of protection under the Privacy Act 1988. This includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation, health or disability status, or criminal record. Personal and sensitive information handled by the College is regulated primarily under the Privacy Act 1988 (Cth), including the APPs
Health Information	A type of sensitive information that relates to an individual's physical or mental health, medical history, or health services provided. This also includes information collected in connection with providing health or wellbeing services at the College. Health information is regulated in Victoria under the Health Records Act 2001 (Vic).

This document is the property of Victory Lutheran College and is not controlled when printed.

28 Drage Road Wodonga Victoria 3690 | 02 6057 5859 | ABN 49 650 193 098 | reception@vlc.vic.edu.au | **www.vlc.vic.edu.au**

5. POLICY

What information does the College collect?

The College may collect personal information including:

a) Student and family information such as, enrolment, contact, health and wellbeing information, and parenting and access arrangements.

b) Staff, volunteer and contractor information such as, qualifications, working with children checks and teacher registration.

c) Visitor and community information

d) Images, audio or video recordings

e) Information generated through use of the College's systems, networks or facilities (including CCTV).

College ICT systems

The College is committed to promoting the safety, wellbeing and appropriate use of digital technologies by students. To support this, the College reserves the right to monitor, access and review student use of its information and communication technology (ICT) systems, networks, devices and platforms. Monitoring may include, but is not limited to, internet usage, email communications, file access, application use, and browsing activities on College-provided accounts and devices.

The College will take steps to ensure that any monitoring is proportionate, conducted in accordance with applicable privacy and child safety laws, and limited to what is necessary to achieve these purposes. Information obtained through monitoring will be handled in accordance with this Privacy Policy and may be disclosed where required to protect the safety and wellbeing of a student or others, or as otherwise permitted or required by law.

By using the College's ICT systems, students and their parents/carers acknowledge and consent to such monitoring for these purposes.

How does the College collect this information?

Information is collected directly from individuals and, where appropriate, from third parties such as government agencies, medical practitioners, previous schools, or service providers.

Collection occurs through forms, interviews and meetings, online systems, communications, and College-approved digital platforms.

The College also provides Collection Notices - *Standard Collection Notice (Student, Parent/Carer/Guardian)* and *Employment Collection Notice* - at the time personal information is collected. These notices explain the purposes of collection, how the information may be used or disclosed, and any relevant legal requirements. Collection Notices should be read together with this Privacy Policy.

Why does the College collect this information?

Primary purposes of collecting information about students and their families

The College collects information about students and their families primarily to provide schooling and support student wellbeing. This includes:

a) educating students

b) support students' social and emotional wellbeing, and health

c) fulfil legal obligations (duty of care, disability adjustments, OHS requirements)

d) communicating with families about school matters, achievements and events

e) managing and administering College operations and programs

f) enabling the College to:
   i. meet reporting, regulatory, planning and funding requirements
   ii. respond to and investigate incidents, safety, security and legal claims

g) security of the College and the College's property

h) supporting College community groups such as the P&F and VOCA

i) supporting College fundraising and marketing activities

If the required information is not provided, the College may be unable to enrol or continue enrolment, or students may be unable to participate in certain activities.

This document is the property of Victory Lutheran College and is not controlled when printed.

Staff, Job Applicants and Contractors

The College collects information about staff, job applicants and contractors primarily to assess and (if successful) engage the applicant, staff member or contractor. This includes:

a) Assess suitability for employment or other roles

b) Meet insurance and legal obligations (including OHS, contract law, child protection)

c) Administer payroll, contracts, and workplace processes

d) Investigate incidents or respond to legal claims

How does the College use or disclose information?

Personal information is used primarily for the purpose for which it was collected and may also be used or disclosed for closely related secondary purposes that individuals would reasonably expect, or where consent has been provided.

The College may use or disclose personal information when:

a) it is required for the primary purpose of collection

b) it is necessary for a related and reasonably expected secondary purpose, including supporting the College Board's functions

c) notice or consent has been given, including for the use and disclosure of enrolment or community information

d) the College believes it is necessary to prevent or lessen a serious threat to a person's life, health, safety, or welfare, or to public health or safety

e) the College is legally required or authorised to do so, including under child protection laws, workplace laws, or where needed to exercise or defend its legal rights

f) disclosure is otherwise permitted under this Policy or relevant legislation, including the Health Records Act 2001 (Vic) for health information.

Sensitive and Health Information

Sensitive and health information is afforded a higher level of protection and is used only for the primary purpose for which it was collected, a directly related purpose, or as otherwise permitted by law.

Health privacy requirements generally apply to health information held about employees and students.

Images and Publications

At certain times throughout the year, students have the opportunity to be photographed or filmed at College events for digital or printed publications, such as the Victory Way, College website, College promotional materials and social media, or to promote the College in local newspapers and other media. Images used publicly require consent (provided upon enrolment), which may be withdrawn at any time by notifying the College in writing.

Third-party service providers

The College uses third-party service providers, including cloud-based systems, to support its operations. Reasonable steps are taken to ensure these providers handle information in a manner consistent with privacy obligations.

Overseas Disclosure

Personal information may be disclosed overseas, such as when using cloud services or participating in international programs. Disclosure occurs only in accordance with the Australian Privacy Principles or with consent.

6. PROTECTION AND STORAGE OF PERSONAL INFORMATION

The College takes reasonable steps to protect personal information from misuse, loss, unauthorised access, modification, or disclosure.

Personal information may be stored in various formats, including:

a) Paper records

b) Electronic records

c) Staff devices (e.g., laptops)

d) Third-party storage systems, including cloud services

This document is the property of Victory Lutheran College and is not controlled when printed.

All records are stored securely in accordance with applicable record-keeping and archival requirements.

Security Measures

To safeguard personal information, the College implements a range of security and governance controls, including:

a) Restricted access to electronic systems and secure physical storage for hard-copy files
b) Role-based access controls across the College
c) Multi-Factor Authentication for core systems
d) Lockable storage for hard-copy documents and restricted staff access
e) Secure premises and physical security measures
f) Up-to-date IT and cyber security systems, policies and procedures and training where required
g) Document security bin for disposal of records containing personal and sensitive information
h) Staff compliance with privacy and security policies
i) Due diligence on third-party service providers, including cloud and identity-verification vendors

The College may also use Privacy Impact Assessments (PIAs) to evaluate third-party software handling personal, sensitive or health information and to identify and manage privacy risks in line with applicable privacy legislation.

Data Retention and Disposal

The College retains personal information only for as long as necessary to fulfil educational, operational and legal requirements. When no longer required—and unless retention is mandated by law—personal information is securely destroyed, deleted or de-identified. Record retention complies with relevant legislative and archival obligations.

7. ACCESSING INFORMATION

Access to and Correction of Personal Information

Individuals have the right under the Privacy Act and Health Records Act to access and request correction of their personal information held by the College, subject to certain exceptions. Requests must be made in writing to the Privacy Officer (privacy@vlc.vic.edu.au). The College may require proof of identity and details of the information sought and may charge a fee for locating and accessing records. If access is refused, the College will provide written reasons.

Students typically access their information through their parents/carers; however, mature students may request access directly. The College may allow a student to exercise privacy rights independently where their maturity or circumstances warrant this.

Access may be denied where disclosure would unreasonably impact the privacy of others, breach the College's duty of care, or otherwise not be in the student's best interests.

Access to Student Information

The College may only release school reports and routine communications to individuals with a legal right to receive them.

In some cases, even authorised representatives may be denied access—for example, where disclosure would not be in the student's best interests, would breach duty of care, contradict a mature minor's wishes, or impact the privacy of another person.

The Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS) permit prescribed organisations, including Victorian schools, to share confidential information to promote child wellbeing or manage family violence risk.

Access to Staff Information

Staff may request access to their personnel file through the Principal or their delegate.

This document is the property of Victory Lutheran College and is not controlled when printed.

8. RESPONDING TO DATA BREACHES

A data breach occurs when personal information is lost, accessed, or disclosed without authorisation. All confirmed, suspected, or potential breaches (including near misses) must be reported immediately to the Privacy Officer (privacy@vlc.vic.edu.au) or a member of the Critical Incident Management Team (CIMT).

Response to a Data Breach

The College will respond to all data breaches in accordance with the *Data Breach Response Plan* in Appendix 1, which includes:

a) Immediate steps to contain the breach

b) A formal investigation using the *Data Breach Investigation Report template* in Appendix 2.

c) Activation of a data breach response team, where required

If the College has reasonable grounds to believe that a breach is likely to result in serious harm to an individual, it is legally required under the Notifiable Data Breaches (NDB) Scheme to notify:

1. The affected or at-risk individual(s), and
2. The Office of the Australian Information Commissioner (OAIC)

Notifications will be coordinated by the Principal or the Privacy Officer.

Notification Requirements

Where a notifiable breach has occurred, the College will:

a) Contain the breach and undertake an investigation

b) Notify the affected individual(s) directly; if direct notification is not possible, publish a statement on the College website or through other appropriate channels

c) Provide a statement to the OAIC detailing the breach and the College's response

If individuals cannot be contacted, the College will take reasonable steps to ensure public awareness of the notification.

Remedial Action

Depending on the nature of the breach, the College may take actions such as:

a) Reviewing and strengthening internal security measures

b) Implementing technical or procedural remediation

c) Updating College policies and staff training

d) Providing additional guidance to affected individuals

Examples of Data Breaches

Examples of incidents that may constitute a data breach include:

a) Lost or stolen laptops, devices, USB drives or paper files containing personal information

b) Unauthorised access to databases, including hacking or internal misuse

c) Staff accessing or sharing personal information without permission

d) Theft of paper records from unsecured bins or storage

e) Personal information sent to the wrong recipient

If You Suspect a Data Breach

If you become aware of or suspect a data breach, you must:

a) Notify the Privacy Officer or a member of the CIMT immediately

b) Report lost or stolen devices, phishing attempts, suspected hacking, or information sent to the wrong individual

9. PRIVACY COMPLAINTS AND ENQUIRIES

The College is committed to managing personal information responsibly and responding promptly to privacy concerns. Individuals who believe their personal information has been mishandled, or who have questions about how the College handles personal information, may make a complaint through the process below.

This document is the property of Victory Lutheran College and is not controlled when printed.

Making a Privacy Complaint

Individuals may lodge a privacy-related complaint by contacting the Privacy Officer (privacy@vlc.vic.edu.au) in writing. Complaints should outline:

a) The nature of the concern

b) The personal information involved (if known)

c) Any relevant details or supporting documentation

Privacy complaints will be managed in accordance with this policy and the College's *Complaints and Conflict Resolution Policy and Procedure*, which outlines broader principles and steps for handling concerns and resolving disputes.

Internal Review Process

Upon receiving a privacy complaint, the College will:

1. Acknowledge receipt within a reasonable timeframe
2. Review the complaint and gather any necessary information
3. Investigate the circumstances, with reference to privacy legislation and internal policies
4. Provide a written response outlining findings and any actions taken

The College endeavours to resolve privacy complaints within 30 days, if more time is needed, the complainant will be informed.

Escalation to the OAIC

If the complainant is not satisfied with the College's response, they may escalate the matter to the Office of the Australian Information Commissioner (OAIC), who can investigate potential breaches of the *Privacy Act 1988 (Cth).*

Office of the Australian Information Commissioner (OAIC)

Online: www.oaic.gov.au

Phone: 1300 363 992

Mail: GPO Box 5218

Sydney NSW 2001

The OAIC generally expects individuals to raise their concern with the organisation first and allow an opportunity for resolution before lodging a formal complaint.

10. COMPLIANCE WITH LAWS

- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Health Privacy Principles contained in the Health Records Act 2001 (Vic) (referred to as "the Health Records Act")
- Child Information Sharing Scheme Vic (CISS)
- Family Violence Information Sharing Scheme Vic (FVISS)

11. RELATED DOCUMENTS

- Standard Collection Notice
- CCTV Privacy Notice
- Employment Collection Notice
- Complaints and Conflict Resolution Policy and Procedure
- Responsible Use of AI Policy and Procedure
- Digital Technologies Policy and Procedure
- Whistleblower Policy
- Data Breach Investigation Report Template

This document is the property of Victory Lutheran College and is not controlled when printed.

12. POLICY ADMINISTRATION

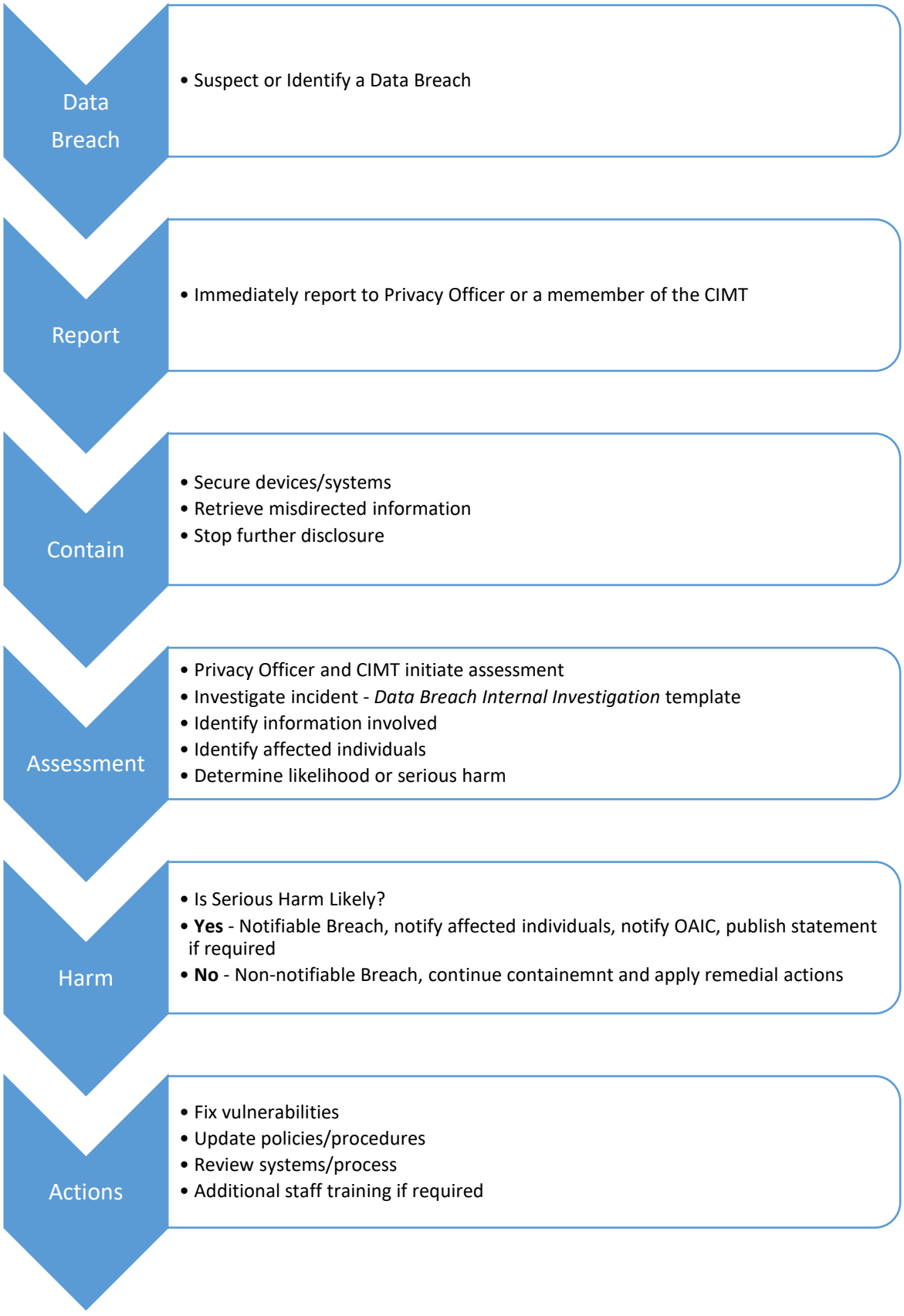
This policy will be reviewed every three years, as new legislation comes into effect or after a significant incident.

Responsible Person/s	Approver	Date Approved	Next Review
Principal	College Board	March 2026	March 2029

Date Updated	Version	Summary of Changes	Updated By
March 2012	1	Policy Update	
June 2016	2	Policy Update	
July 2016	3	Policy Update – minor amendments	
July 2021	4	Policy review and approved	
August 2025	5	Transferred to new policy format	Risk & Compliance Officer
March 2026	6	Reviewed in accordance with the Department, ISV and LEVNT. Reviewed and approved by the College Board.	Risk & Compliance Officer
July 2026	7	Updated legislative references to reflect applicable Commonwealth and Victorian privacy legislation for independent school.	Risk & Compliance Officer

This document is the property of Victory Lutheran College and is not controlled when printed.

APPENDIX 1 - DATA BREACH RESPONSE PLAN



This document is the property of Victory Lutheran College and is not controlled when printed.

APPENDIX 2 - DATA BREACH INVESTIGATION REPORT TEMPLATE

Meeting Date:

Data Breach Response Team:

Incident Overview	
Date of Report	
Reported By	
Date of Breach	
Summary of Incident	*A concise overview of what occurred.*

Description of the Data Breach	
Type of Breach *(select all that apply)*	*Unauthorised access* *Unauthorised disclosure* *Loss of data/device* *Ransomware/malware* *Other, specify*
Description of the Event	*Detailed timeline of events leading up to the breach.*
Systems, Applications or Tools Involved	
Location of Compromised Data	*eg server, email, USB device*

Category and Sensitivity of Data Affected	
Types of Personal or Sensitive Data Involved, *(select all that apply)*	*Names* *Contact details* *Financial information* *Health information* *Identification documents* *Credentials/passwords* *Company confidential information* *Other (specify)*
Data Classification Level	*Public* *Internal* *Confidential* *Highly Confidential / Sensitive*
Estimated Volume	

This document is the property of Victory Lutheran College and is not controlled when printed.

Individuals or Groups Affected	
Internal Stakeholders	
External Individuals or Organisations	
Number of Individuals Potentially Impacted	

Immediate Actions – *list all steps taken to isolate the incident and prevent further exposure.*

Investigation Findings	
Root Cause Analysis (RCA)	*Identify underlying cause eg human error, system vulnerability, policy gap*
Contributing Factors	*Investigation summary – clear explanation of how and why the breach occurred*

Impact Assessment	
Legal & Compliance Impact	*(Privacy laws, contractual obligations, regulatory concerns)*
Operational Impact	*Describe any downtime, service disruption, or business effect.*
Reputational Impact	*Effect on trust, clients, staff, or public perception.*
Financial Impact	*Details of actual or potential cost.*
Impact Rating	*Low, Medium, High, Severe*

Notification Requirements	
Regulatory Notification Needed?	Yes / No *If yes, authority, deadline, responsible person*
Individuals/Clients Notified?	Yes / No *Communication method*
Internal Notifications	Yes / No *Who and how*

Corrective Actions – *list actions to be taken and by who*	
Action/s	**Who**
1. Determine Severity of Harm and if data breach can cause serious harm to individuals	
2.	
3.	
4.	

This document is the property of Victory Lutheran College and is not controlled when printed.

5. Review Privacy Policy	
6. Training, upskilling – Y/N	

Other

This document is the property of Victory Lutheran College and is not controlled when printed.