Lowther Hall

ANGLICAN GRAMMAR SCHOOL

All about the girl

Privacy Policy

Date of last review:	2021
Review cycle & approval responsibility:	Annual – Privacy Committee 3 yearly - Executive & School Council
Category:	Privacy
VRQA required:	Yes
Locations:	O:Drive, LowtherLink, BoardPro, Website

PRIVACY POLICY

1. PURPOSE AND CONTEXT

Lowther Hall Anglican Grammar School is committed to managing personal information in accordance with all relevant Commonwealth and Victorian laws and best practice. The School is required to comply with the Australian Privacy Principles contained in the Privacy Act 1988 (Cth) as amended and the applicable State health privacy legislation (including the Victorian Health Records Act 2001).

This Policy sets out the approaches used by Lowther Hall Anglican Grammar School ("the School") in the management of personal information and the steps to be taken to seek to be compliant with the relevant legislation.

Privacy matters, including the development and review of privacy policies, processes and breaches, are overseen by the School's Privacy Committee which, in turn, reports to the School Council via the Governance and Strategy Committee.

In the daily operations of the School it is generally expected that information shared in conversations, activities or in writing would not be passed on to others unless it was publicly delivered or clearly intended for broader circulation.

2. DEFINITIONS

Child Information Sharing Scheme (CISS)

The CISS was established by the Victorian Government in 2018 and applies to all Victorian schools and early childhood education and care services. The Scheme enables organisations to share confidential information (defined as health and personal information) to promote the wellbeing and safety of children. Schools can request and/or disclose confidential information which meets all of the threshold requirements.

Family Violence Information Sharing Scheme (FVISS)

The FVISS enables organisations to share information for the purpose of assessing or managing family violence risk. If the School suspects that a child is at risk of family violence, the School may be required to share information with other organisations in compliance with both the FVISS and the CISS.

Office of the Australian Information Commissioner (OAIC)

The Office of the Australian Information Commissioner is an independent agency within the Attorney-General's portfolio whose purpose is to promote and uphold privacy and information access rights. The OAIC has a range of regulatory responsibilities and powers under the Privacy Act 1988 (Privacy Act), the Freedom of Information Act 1982 (FOI Act) and other legislation.

Parents and caregivers

In this policy, the terms parents, caregivers and/or guardians are used interchangeably and include people or entities who are not parents or guardians but who are party to the enrolment contract by which a student is enrolled at the School.

Privacy Impact Assessment (PIA)

PIA means a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact.

Privacy and confidentiality

The terms "privacy" and "confidentiality" are understood differently.

- Privacy is regulated by the Privacy Act 1981 (Cth) and the Australian Privacy Principles ("APPs"). States and Territories have their own legislation also. These privacy laws govern the **handling of personal information** about individuals and how it is collected, held, used and disclosed.

- Confidentiality means the passing or holding of **information which has been conveyed in confidence**, which is not readily available publicly. There is no specific confidentiality legislation in Australia. Confidentiality, and breaches thereof, are beyond the scope of this Policy. Issues pertaining to confidentiality can be raised with any member of the School's Executive Team.

Staff

Staff includes teaching, administration and support staff, permanent and casual staff, contractors, coaches, volunteers, teacher candidates, trainees and work experience students.

3. SCOPE

This policy applies to all members of the Lowther Hall community including staff, students, parents, caregivers, school council members, volunteers, contracted parties and third-party providers.

Privacy matters pertaining to photography and film are covered by the Photography and Video Policy and this Policy should be read in conjunction with it.

4. COLLECTION AND HOLDING OF PERSONAL INFORMATION

The School collects and holds personal information, including sensitive information, about the following parties:

- Students, parents, caregivers and/or guardians
  - The School will collect and hold personal information, including sensitive information, relating to the above parties before, during and after the course of a student's enrolment at the School.
- Prospective students and families
- Past students (Old Grammarians)
- Job applicants, staff members and volunteers
- Suppliers and independent contractors
- Parties/businesses who donate funds or gifts towards the School's fundraising ventures/events
- Other people who come into contact with the School.

4.1 The kinds of personal information the School collects and holds

The kinds of personal information the School collects and holds depends on the type of dealings a party has with the School. It may include sensitive personal information. The information includes (but is not limited to):

- Names, family details, date and country of birth, nationality, religious denomination, test and other data, including biometric data
- Health and special needs information
- Photographs, film and other visual images capable of being stored electronically (further information regarding photographs and film are set out in the Photography and Video Policy)
- Contact details and addresses
- Employment history, qualifications, police record and references
- Information the School is authorised or required by or under Australian law to collect or to satisfy its legal or regulatory obligations
- Court Orders

At times, the School may collect additional information in order to reduce specific risks that arise.

4.2 Sensitive Personal Information

The information referred to above may include sensitive personal information. Sensitive personal information will only be collected where it is necessary to do so and will be used, held and disclosed in the circumstances referred to above where (a) consent has been provided (which may be implied in certain circumstances), or (b) such use, holding and disclosure is reasonably to be expected or is necessary to enable the School to satisfy its legal obligations or is otherwise permitted by law.

4.3 How the School collects personal information

The School collects personal information in ways that include (but are not limited to) information obtained:

- In the course of the enrolment process
- From face to face meetings
- Over the telephone and internet (including email)
- During the school year by way of forms filled out electronically or manually by parents and/or guardians and students
- Through the School's intranet portal
- From third persons such as medical practitioners and health professionals, lawyers and other legal personnel
- From prospective employees through the recruitment process, at interviews, from past employers and referees, or from a prospective employee's recruitment agent
- When taking photographs, films or other digital visual images
- From volunteers and contractors through our engagement process.

4.4 Personal information derived from students

There may be occasions when the School collects personal information about students directly from them, such as when a student attends a school counsellor, teacher, or pastoral care provider.
Students will also be required to provide a photograph of their image for their School ID card, for publication in The Chronicle and on the School websites and for other displays throughout the School campus.

4.5 How the School holds and manages personal information

4.5.1 Managing information

The School takes all reasonable steps to protect the personal information it holds from misuse, interference and loss and from unauthorised access, modification or disclosure. This is done through the use of:

- Locked storage and locked offices for paper records
- Security and password protected access rights to electronic records.

The School will take all reasonable steps to ensure that any personal information held by it is up-to-date, complete, relevant, not misleading and accurate.

Further, the School's staff is under a contractual obligation to maintain confidentiality in relation to confidential personal information held by the School.

4.5.2 Managing information relating to job applications

Any personal information held in relation to an unsuccessful job application will be destroyed by the School unless an applicant consents to it being held for future positions that may arise.

4.5.3 Managing information stored on cloud servers

Before a Cloud service is used by the School, either directly or indirectly, the School makes sure that the company used is compliant with Australian Privacy laws (state and federal) and standards in their letter of engagement.

5. THE PURPOSES FOR WHICH THE SCHOOL USES PERSONAL INFORMATION

5.1 Students, parents or guardians

The School collects, holds, uses and discloses personal information for the primary purpose of enabling the School to provide schooling for the student. This includes satisfying both the needs of parent, the needs of the student and the needs of the School community as a whole, before, during and after the course of a student's enrolment at the School.

The purposes for collecting, holding, using and disclosing personal information of students, parents or guardians also include (but are not limited to):

- Keeping parents and/or guardians, staff and students informed about matters relating to the student's education and welfare
- Assisting with the administration of the School's operations, including its before and after school programs
- Looking after the education, safety, care and wellbeing of students
- Seeking donations and fundraising assistance for the School
- Satisfying the School's legal obligations as an educational institution in Victoria and to discharge its duty of care to its students
- Maintaining records of the School's past and present students
- Recording and celebrating student academic, sporting, musical, theatrical and other achievements, student activities and other news in the School newsletters, magazines, website and on its digital social media platforms
- Assisting in the promotion of the School
- Communicating and engaging with members of our School community, past and present.

5.2 Prospective students and families

The purposes for collecting, holding, using and disclosing personal information of prospective students and families include (but are not limited to):

- Reviewing an application for a student's enrolment
- Assisting with the administration of the School's operations
- Communicating and engaging with members of our School community, past and present.
- Preparing for the education of students

5.3 Job applicants and staff members

The purposes for collecting, holding, using and disclosing personal information of job applicants and staff members include (but are not limited to):

- Maintaining historical records of the School's past and present staff
- Assessing applicants for prospective employment or engagement as contractors
- Assisting with the administration of the School's operations
- Enabling the School to comply with its legal obligations as an educational institution and to discharge its duty of care to its students.
- For insurance purposes, such as public liability or Workcover
- Fundraising or promotion of the School
- Investigating incidents or defending legal claims about the School, its services or staff
- Providing a reference

5.3.1 Exception in relation to employee records

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 an employee.

5.4 Volunteers

The purposes for collecting, holding, using and disclosing personal information in relation to volunteers who assist the School in its functions or who conduct associated activities such as PFA (Parents' and Friends' Association), LHOGA (Lowther Hall Old Grammarians Association), FOR (Friends of Rowing), FOM (Friends of Music) include but are not limited to:

- enabling the School and the volunteers to work together
- for insurance purposes
- to satisfy the School's legal obligations.

5.5 Suppliers and independent contractors, parties/businesses (who may donate funds or gifts towards the School's fundraising ventures/events, and other people who come into contact with the School):

The purposes for collecting, holding, using and disclosing personal information in relation to the above parties include (but are not limited to):

- enabling them and the School to work together
- for insurance purposes
- to satisfy the School's legal obligations
- seeking funds and marketing for the School.

5.6 Promotion of and fundraising for the School

Promotion and fundraising for the future growth and development of the School is an important part of ensuring that the School continues to be a quality learning environment. The information collected by the School may be used to make an appeal on behalf of the School.

School publications such as Lowther News, The Chronicle, general newsletters, circulars and other magazines and platforms such as LowtherLink, which include personal information, may be used for marketing purposes.

From time to time the School uses photo images or video recordings of students as part of its marketing activities. Photos and video recordings are covered by this Privacy Policy as well as the School's Photography and Video Policy.

Any requests not to receive direct marketing from the School may be made to the Privacy Officer, contact details for whom are set out below.

6. TO WHOM THE SCHOOL MIGHT DISCLOSE PERSONAL INFORMATION

6.1 In conducting its operations, the School may from time to time disclose certain personal information to:

- Parents and/or guardians
- Staff
- Coaches and volunteers
- Competition organisers
- Third-party providers such as official school photographers
- Organisations running Scholarship exams
- People providing services to the school such as specialist visiting teachers
- Camp providers
- Excursion providers and providers hosting offsite events
- Old Grammarians
- Publishers of School related material
- Insurance companies
- Travel agents and associated travel, transport, and accommodation providers
- Medical practitioners and other providers of health or wellbeing services
- Government departments and agencies including the Department of Health and Human Services
- Anyone to whom you authorise the School to disclose information.
- Anyone to whom the School owes a legal obligation to disclose information
- Other schools and educational providers
- Host families in other schools
- To legal practitioners for the purpose of receiving legal advice
- To Courts, including the Family Courts pursuant to a subpoena or other Court Order.

Where necessary, this information may include sensitive information. In this case, the School will usually take reasonable steps to gain consent to disclose the information.

6.2 Child Information Sharing Scheme (CISS)

The Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS) apply to all Victorian schools. The School will request access to and disclose confidential information with other information sharing entities (ISEs), providing it meets the threshold requirements.

All of the threshold requirements must be met before sharing confidential information. These include:

- the purpose of sharing information is to promote the wellbeing and safety of a child;
- the information may assist the organisation to make a decision, assessment or plan, conduct an investigation, provide a service or manage any risk in relation to a child; and
- the information is not 'excluded information' under the CISS.

The process for disclosing information under the CISS or FVISS is set out in **Appendix A**.

6.3 Parents and caregivers' consent to have their personal information shared to other parents

The School will disclose personal information (name, email address and phone number) of parents and caregivers to other parents and caregivers only if their consent is given.

6.4 Mandatory Reporting

The School will disclose personal information where it is required to fulfil Mandatory Reporting obligations.

6.5 Credit providers

The School will not provide information to credit providers unless specifically authorised to do so.

6.6 Sending information overseas

The School will only disclose personal information to an overseas recipient if it is necessary to do so, such as when storing personal information with "cloud" service providers situated outside Australia, or to facilitate a school exchange program, trip/tour or partnership.

The School will not send personal information about an individual outside Australia without the consent of the individual or without being satisfied that the overseas entity is subject to the Australian Privacy Principles or other substantially comparable privacy legislation.

6.7 Year 12 VCE results

The Victorian Curriculum and Assessment Authority requires all Year 12 VCE students to elect their preferences regarding their results and privacy. The School strictly adheres to these preferences.

7. ACCESSING PERSONAL INFORMATION

7.1 Access to information

A person may seek access to personal information collected about them and, in the case of parents and/or caregivers, about a student in their care, by contacting the School. The School may ask a person to show proof of identity and to verify a connection to a person whose information is being sought, before providing information and is entitled to charge a reasonable fee for the provision of such information.

7.2 Refusal of Access

There will be occasions when it may be lawful for the School to refuse a person access to their personal information or for the School to deny access to the parent and/or guardian without the consent of the student. Such occasions might include where the release would have an unreasonable impact on the privacy of others or where release may result in a breach of the School's duty of care to the student.

7.3 Release of information to students

There may also be occasions when the School is obliged to provide an older student with access to her own personal information without the consent of her parents and/or caregivers.

7.4 Information regarding third parties

If a parent, caregiver or student provides the School with the personal information of others, such as doctors or emergency contacts, they should inform the third party that this information has been disclosed to the School and why, that they may access that information if they wish to and that the School does not usually disclose the information to third parties.

7.5 Requesting access

Requests to access or correct personal information can be made via the Privacy Officer at the School.

The Privacy Officer
Lowther Hall Anglican Grammar School
PO Box 178
Essendon Vic 3040 Email to: privacy@lowtherhall.vic.edu.au

8. THIRD PARTIES

8.1 School's use of third parties

Where the School uses a third party to collect personal information, the School will take all reasonable steps to satisfy itself that the third party is compliant with Australian Privacy Principles and other relevant legislation.

8.2 Staff engagement with third parties

Where the School requires staff, students or parents to engage with a third party for a school related purpose, the School will take all reasonable steps to satisfy itself that the third party is compliant with Australian Privacy Principles and other relevant legislation.

8.3 Privacy Impact Assessment (PIA)

When engaging with a third party or implementing a new system through which personal information is collected, the School will take all reasonable steps to undertake a PIA, as recommended by the OAIC. This process is set out in **Appendix B**.

9. DATA BREACHES

In the event of a data breach, the School's Data Breach Response Process will be followed. **Refer Appendix C** for a summary of the process.

10. COMPLAINTS

If a member of the School community considers that the School has breached the Australian Privacy Principles the following process should be followed:

(a) Forward a written complaint to the Privacy Officer [email: privacy@lowtherhall.vic.edu.au] setting out the full details of the alleged breach.
(b) The Privacy Officer will consider the matter and make a determination within 45 days of receipt of the complaint. Written advice of the determination will be provided.
(c) If the Privacy Officer determines that there has been a breach by the School of the privacy principles, the Privacy Officer will inform the relevant persons at the School in writing of any action required to remedy the breach. If the breach is not remedied within 30 days the Privacy Officer is required to inform the Principal of the School.

The Privacy Officer will keep a record of all complaints and determinations together with a record of the action taken to remedy such breaches.

11. COMMUNICATION

The Privacy Policy will be communicated to staff as part of their induction process.

It will be made available to parents, caregivers, legal guardians and parties to the enrolment contract on enrolment.

It will be communicated to all staff as part of the three-yearly update.

12. RELATED POLICIES

1. Acceptable Use of Information Technology Policy
2. Copyright Policy
3. Photography and Video Policy
4. Record Management Policy
5. Recruitment Policy

13. REVIEW

This policy is monitored annually by the Privacy Committee to take account of new laws and technology as well as changes to School policies and practices. It is officially reviewed by the Executive Team every three years.

APPENDIX A

PROCESS TO FOLLOW WHEN A REQUEST TO SHARE INFORMATION HAS BEEN RECEIVED

Step 1: Check that the organization seeking the information is an 'Information Sharing Entity' (ISE) referred to in the ISE List. If the organisation is not an ISE, that organisation is not entitled to receive the information requested under the CISS.

Step 2: Assess whether the information meets all of the threshold requirements.
If the information meets the threshold requirements, the school **must** share that information securely (eg by using password protection) and within a reasonable time period.

If the information does not meet the threshold requirements, the school must provide a written explanation to the organisation explaining why.

The school may request further information from the organisation about the information which is being sought, to assist the school to determine about whether the threshold requirements have been met.

Step 3: Notify the child and the parents/guardians about the request for information if it is appropriate, safe and reasonable to do so. This should be done each time an information sharing request is received by the school.

Step 4: Consider any views expressed by the child and parents/guardians in relation to the information sharing request.

Step 5: Comply with all applicable reporting obligations which will continue to apply.

Step 6: Keep detailed written records.

Liability of staff members

Staff members who are authorised to share information under the CISS and who act in good faith and with reasonable care when sharing information will:

- not be held liable for any criminal, civil or disciplinary action for sharing information; and
- not be in breach of any code of professional ethics or considered to have departed from any accepted standards of professional conduct. [*Child Wellbeing and Safety Act 2006* (Vic) s 41ZB].

APPENDIX B

Australian Government
Office of the Australian Information Commissioner

10 steps to undertaking a privacy impact assessment

When developing or reviewing a project, consider the need for a privacy impact assessment (PIA). A PIA identifieshow a project can have an impact on individuals' privacy and makes recommendations to manage, minimise or eliminate privacy impacts.

We recommend that organisations conduct PIAs as part of their risk management and planning processes. While each project is different, a PIA should generally include the following 10 steps.

1. Threshold assessment

Ask if any personal information will be collected, stored, used or disclosed in the project. If the answer is yes, a PIA is usually necessary. Keep a record of this threshold assessment.

2. Plan the PIA

Consider the scope of your assessment, who will conduct it, the timeframe, budget and who will be consulted.

3. Describe the project

Prepare a project description to provide context for the PIA project. This should be brief, but sufficiently detailed to allow external stakeholders to understand the project.

4. Identify and consult with stakeholders

Identify the project stakeholders. Consulting them can help to identify new privacy risks and concerns, better understand known risks, and develop strategies to mitigate all risks.

5. Map information flows

Describe and map the project's personal information flows. Detail what information will be collected, used and disclosed, how it will be held and protected, and who will have access.

6. Privacy impact analysis and compliance check

Critically analyse how the project impacts on privacy. Consider compliance with privacy legislation and any other information handling obligations that may apply to your organisation. Even if the project appears to be compliant with privacy legislation, there may be other privacy considerations that need to be addressed such as community expectations.

7. Privacy management — considering risks

Consider options for removing, minimising or mitigating any privacy risks identified through the privacy impact analysis.

8. Recommendations

Make recommendations to remove, minimise or mitigate the risks identified through the privacy impact analysis. Include a timeframe for implementing the recommendations.

9. Report

Prepare a report that sets out all the PIA information. It should be a practical document that can easily be interpreted and applied. The OAIC encourages the publication of PIA reports and has developed a PIA tool to help you conduct a PIA, report its findings and respond to recommendations.

10. Respond and review

Monitor the implementation of the PIA recommendations. A PIA should be regarded as an ongoing process that does not end with preparation of a report. It is important that action is taken to respond to the recommendations in the report, and to review and update the PIA, particularly if issues arise during implementation.

See our Guide to undertaking privacy impact assessments, e-learning course and PIA tool for more information.

OAIC

APPENDIX C

Data Breach Response Process – Risk assessment factors

Report prepared by:	Name: Date: Role: Privacy Officer contact email: Privacy@lowtherhall.vic.edu.au
Brief summary of data breach	
1. What are the circumstances of the breach	• How did it happen? • When did it happen? • When was it discovered? • Who discovered it? • How was it discovered? • How was the School notified? • Was the breach internal or external?
2. What is the type, nature and amount of personal information involved in the breach	• Who is affected by the breach? • Who is the information about? • What kind/s of information is involved? • How sensitive is the information? • How many people are affected (approximately)? • Who has gained unauthorised access to the affected information?
3. Is the personal information adequately encrypted, anonymised or otherwise not easily accessible	• Is the information rendered unreadable by security measures or whether the information is displayed or stored in ways that renders it unusable if breached? • How likely could the information be used to identify an individual, a School or others?
4. What is the potential harm for the affected individuals	• How could the information be used? • What type of harm could result?
5. Is there evidence of intention to steal the personal information	• Where a device has been stolen, can it be determined whether the thief specifically wanted the information on the device, or the device itself? • Is there any evidence of intention to cause harm by the breach? • Did it involve malicious behaviour or was it a processing error, such as emailing a student list to an unintended recipient?
6. Can the information be recovered	• Has a lost or stolen device been found or returned? • Has the information been recovered or restored? • Is there evidence that it has been accessed, copied or tampered with?

7. What action has been taken to contain, control or mitigate the breach or the harm	• Have you attempted to recover the information, shut down or suspend the affected services, website or online platforms, revoked or changed access passwords, etc? • What further steps (if any) are required?
8. Is there a risk of ongoing breaches or further exposure of the information	• What is the risk of recurrence of this type of breach? • Is this a systemic problem or an isolated incident?
9. Have there been other breaches that could have a cumulative effect	• Is this an isolated incident? • Does the cumulation of other breaches of personal information form the basis to cause serious harm? • What other systems have been compromised?
10. Are the affected individuals aware that the breach has occurred	• How and who will make contact? • If the breach is as a result of a third party, how will contact be made? • Does a standard letter need to be sent to affected parties?
11. Who has been notified or needs to be notified about the breach	• Privacy Committee • OAIC • Legal agencies • Police • Affected individuals
12. What changes will be implemented to prevent or reduce the risk or a reoccurrence	• What safeguards or measures were in place to prevent a breach of this nature occurring. Why given these safeguards, did the breach occur? • What additional or amended measures will need to be implemented, such as policies, privacy and security audit/s, improved physical security or technical requirements?
13. Who is the contact concerning the breach	• Name, position, phone and email address of the person within the School for any further enquiries • Is there a separate contact for media enquiries?

Version 3.0

Date: 12 May 2021

SAMPLE LETTER

APPENDIX 1

DATE

Dear [name]

On [date] we alerted you to a suspected data incident.

I can now update you that, with the assistance of market leading IT forensic experts, the School has found that your information on one of our databases was unlawfully accessed by an external party on [date].

While our independent investigation found that no passwords were compromised, the database includes information about community members who may have made donations and payments, and/or accessed third party platforms through the School's portals.

The information about you that was contained in the database that was accessed included some or all of the following, depending on what you had provided:

- Name
- phone number
- address
- email
- date of birth and
- payment history.

We are contacting you directly so that you can take simple and immediate steps to protect your information and avoid any potential scams.

Given the nature of your information in the database that was accessed, you may meet a greater risk of scam activity. This may come in the form of emails, text messages or phone calls. We recommend that you remain vigilant and refrain from actioning unsolicited requests to provide information or clicking on links or attachments. Scammers can seem quite believable and do impersonate government, businesses and charities. If in doubt about a communication, I encourage you to make your own enquiries first before responding.

Lowther Hall has notified industry regulators, including the Office of the Australian Information Commissioner and Australian Cyber Security Centre. The matter has also been reported directly to police authorities.

We take the privacy and the protection of school community members' information very seriously and I sincerely regret this has happened.

I assure you we have taken important steps working with our IT experts to further bolster the security of our technology systems to help prevent any similar incidents happening again.

You can access more information on our website.

If you would like to seek or provide more information on this matter, please contact our Privacy Officer on 9325 5000 or email privacy@lowtherhall.vic.edu.au

Yours sincerely,

Elisabeth Rhodes
Principal