



**Overnewton**  
Anglican Community College

# Privacy Policy



# Contents

<b>Privacy Policy Overview</b>	<b>2</b>
Purpose	2
Scope	2
Policy Statement	2
<b>Policy Implementation</b>	<b>2</b>
1. Collection	2
2. Use and Disclosure	4
3. Management of Information	6
4. Data Breaches	7
5. Complaints Resolution	7
6. Contact Information	7
<b>Policy Status and Review</b>	<b>8</b>
Document Details	8
Version Control	8
<b>Appendix A</b>	<b>9</b>
<b>Appendix B</b>	<b>10</b>

# Privacy Policy Overview

## Purpose

This policy outlines the processes followed by Overnewton Anglican Community College (the College) to collect, use, disclose, store, and dispose of personal information provided or collected.

The College is bound by the *Australian Privacy Principles* (APPs) in the *Privacy Act 1988* (Cth) (Privacy Act). Internal policies and procedures have been adopted to ensure personal information that the College collects, stores, uses and discloses is handled and managed in accordance with the APPs and the Privacy Act.

The College may review and update this Privacy Policy to ensure new laws and technology, and changes to the College's operation, practices, and environment are considered.

## Scope

This Policy applies to all College staff, parents/guardians, volunteers, contractors, and other community stakeholders.

## Policy Statement

This policy explains how the College collects and manages personal and health information, including sensitive information, consistent with Australian Privacy Law and other associated legislation.

# Policy Implementation

## 1. Collection

The College collects personal information as outlined below.

### 1.1. Personal Information Collected by the College

The College may collect personal information about employees or others (such as minors under their care), including:

- contact details such as names, next of kin, addresses and phone numbers.
- identification documents and information, including residency status and date of birth.
- general personal information, such as images (e.g., photographs and videos), academic results and performance, and health matters; and
- other sensitive information.

The College may collect this information to identify:

- students and parents/guardians of students before, during and after the course of a student's enrolment at the College.
- job applicants, staff members, volunteers and contractors; and
- other people who are involved with the College.

The College may also collect personal information which is:

- 'sensitive information', including information relating to nationality, racial or ethnic origin, religious beliefs or affiliations, criminal record, genetic or biometric information; and
- 'health information' (particularly for students, parents, guardians, employees and other visitors to the College premises), including medical records, disabilities, allergies, immunisation details and psychological or counselling records.

The APPs permit the College to collect sensitive information:

- for the purposes of its functions and activities, which includes providing education and community services.
- when the individual, or their parent/guardian, has consented.
- when collection is required or authorised by law, which includes the common law duty of care; and
- where the College reasonably believes the collection is necessary to lessen or prevent serious threat to the life, health, or safety of any individual or the public.

When required, and it is practicable to do so, the College will seek consent before collecting sensitive and/or health information and provide the purpose for doing so.

## 1.2. Process for Collecting Information by the College

Unless unreasonable or impractical, the College will collect personal information directly from the individual concerned or their parent/guardian:

- by way of completed forms and questionnaires.
- during face-to-face meetings, interviews, telephone calls, video conferences.
- via the College website or digital operating system/platform.
- during other interactions.

At times, use of CCTV cameras located at the College premises may be used to gather information.

On occasions, a third party may provide information to the College, such as a report provided by a medical professional, therapist or another school. Where circumstances permit, the College will seek an individual's consent (or parent's/guardian's consent) before obtaining personal information from third parties.

### 1.2.1. Required Personal Information Not Provided

The enrolment of a student or the educational and/or other services provided by the College may not continue if the requested personal information is not provided to the College.

**Employee records exception:** Under the Act, the APPs do not apply to a private sector employee record. As a result, this Privacy Policy does not apply to the College's management of employee records, where the management is directly related to a current or former employment relationship between the College and employee.

### 1.2.2. Unsolicited Information

In some instances, the College may be provided with or otherwise receive personal information without having sought it through the above means of collection (**Unsolicited Information**). This may include receipt by:

- misdirected correspondence, including by postal, personal, or electronic delivery; and
- employment, contracting or volunteer applications which do not relate to an advertised vacancy.

Where the College receives Unsolicited Information, it will determine whether the personal information could have been collected by soliciting it from the individual (as above). Where the College concludes that the Unsolicited Information is not of a nature which would ordinarily be requested or collected by the College, it will, where lawful and reasonable to do so, destroy the Unsolicited Information or ensure it is otherwise de-identified. If the College decides to retain the Unsolicited Information, it will manage this personal information in accordance with this Privacy Policy.

### 1.2.3. Anonymity and Pseudonymity

There is the option of not being identified or of using a pseudonym when working with the College in relation to a matter. However, if the preference is to not provide personal information to the College it may inhibit or be impractical to provide education or other products or services to the family or student.

## 2. Use and Disclosure

### 2.1. Use of College Personal Information Collected

The College will use the personal information collected for,

- the primary purpose for which it was collected, and
- such other related purposes that would be reasonably expected or implied under the same consent.

The College may also use personal and sensitive information for a secondary purpose where:

- the use of disclosure is required or authorised by or under any Australian law or a court/tribunal order.
- it is a permitted health situation, such as sharing with medical professionals.

#### 2.1.1 Students and Parents/Guardians

In relation to personal information of students and parents/guardians, the College's primary purpose of collection is to enable the College to provide education services to the student, exercise its duty of care, and perform necessary associated administrative or community activities which will enable students and parents/guardians to engage in all activities of the College. This includes satisfying the needs of the parents/guardians, the needs of the student and the needs of the College throughout the entire period in which the student is enrolled at the College.

The secondary purposes for which the College may use personal information of students, parents/guardians include:

- ensuring parents/guardians are informed about matters relating to their child's education, through correspondence, newsletters, and magazines;
- facilitation of day-to-day administration;
- attending to students' educational, social, and medical wellbeing;
- seeking donations and marketing;
- satisfying any legal obligations;
- enabling the discharge of duty of care.

#### 2.1.2 Job Applicants, Staff Members and Contractors

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

The secondary purposes for which the College uses personal information of job applicants, staff members and contractors include:

- administration of the individual's employment or contract.
- regarding insurance matters.
- seeking donations and marketing.
- satisfying any legal obligations:
- enabling the discharge of duty of care.

#### 2.1.3 Volunteers

The College obtains personal information about volunteers who assist the College in its functions or conduct associated activities.

#### 2.1.4 Marketing and Fundraising

The College treats marketing and seeking donations for the future growth and development of the College as an important part of ensuring that the College continues to be a quality learning environment in which both students and staff thrive.

Parents/guardians, staff, contractors, and other members of the wider College community may receive fundraising information. College publications, such as *Whispers* and the annual College magazine *Omnia*, which include photographs and personal

information, may be used for marketing purposes. Such publications, or extracts from them, may be posted on the College website. There is an opt-out option for any member of the community that does not want personal information included in College publications. This also applies to the receipt of marketing and fundraising activities. Such requests are to be made via the College Privacy Officer. Contact details for our Privacy Officer appear at the end of this policy.

## 2.2. Disclosure of Personal Information by College

The College may disclose personal information, including sensitive information, held about an individual for educational, community, administrative and support purposes to:

- another school;
- government departments (including for policy and funding purposes);
- medical practitioners;
- providers of educational, support and health services to the College, including visiting specialist teachers, activity provider and sports coaches;
- providers of learning and assessment tools;
- assessment and education authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and National Assessment Program – Literacy and Numeracy (NAPLAN) Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- organisations providing administrative, technology and financial services to the College;
- recipients of College publications such as Whispers, and the College magazine Omnia, including via the College website: [www.overnewton.vic.edu.au](http://www.overnewton.vic.edu.au);
- parents/carers;
- any parties to whom signed consent has been provided;
- any parties to whom authorised disclosure of information by law is mandated including child protection laws.

The College will take reasonable steps to ensure that the personal information that is collected, used and disclosed is accurate and up-to-date. The College will immediately update its records when an individual provides any new information or information that has changed.

## 2.3. Child Information Sharing Scheme (CISS)

The Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS) apply to all Victorian schools.

Where the College determines that insufficient information is available to effectively support a student's wellbeing or safety, they can use the schemes to request and proactively share information with authorised services. The schemes enable schools and other prescribed ISEs to access and share relevant information with each other to promote the wellbeing or safety of children and to assess or manage family violence risk.

The College 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;
- 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**.

## 2.4. Mandatory Reporting

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

## 2.5. Sending and Storing Information Offsite

The College may disclose personal information about an individual to overseas recipients, for example, to facilitate an international tour. However, the College will not send personal information about an individual outside Australia unless:

- consent of the individual, their parent or guardian is obtained (in some cases this consent will be implied).
- it is legally authorised or required to do so; or
- it otherwise complies with the APPs or other applicable privacy legislation.

The College may also use other online or 'cloud' storage providers to store personal information and to provide online services to the College that involve the use of personal information, such as services relating to email, instant messages and education and assessment applications.

Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's server which may be situated outside Australia.

## 3. Management of Information

### 3.1. Management and Security of Personal Information

The College will take reasonable steps to protect the personal information that is held from misuse, loss, unauthorised access, interference, modification, destruction, disclosure, or accidental loss by use of various methods including locked storage of paper records and pass-protected access rights to computerised records.

The College's staff are required to respect the confidentiality of personal information and the privacy of individuals.

If there is unauthorised access to, disclosure of, or loss of personal information where unauthorised access or disclosure is likely to occur, the College is required to notify the individuals to whom the information relates that such a breach has occurred. This requirement is limited to circumstances where the College determines that a reasonable person would conclude that access to, or disclosure of, personal information would likely result in serious harm to any individuals to whom the information relates. Where it is not practicable to notify each individual to whom the information relates, the College will contact anyone that has been impacted by detailing the breach or likely breach, including any recommended steps that the relevant individuals should take.

Where personal information is no longer required for an authorised purpose, the College will take reasonable steps to destroy or permanently de-identify the personal information.

### 3.2. Access and Updating Personal Information

Under the Privacy Act, an individual generally has the right to seek and obtain access to any personal information which the College holds about them and to advise the College of any perceived inaccuracy. There are some exceptions to this right set out in the Privacy Act, including access to employee records. Students will generally be able to access to personal information through their parents/guardians, older students may seek access themselves.

Parents/guardians may send a request to the College to update their personal details. The College requires notification of any changes to held personal information to ensure it is accurate, complete, and current. Any personal information is deemed to not need amendment, annotation will reflect this on College files.

Any request to access information or update personal information is to be directed to the College's Privacy Officer in writing.

Verification of identity may be required to verify individual identity and specify what information is required. The College may charge a reasonable fee to cover the cost of verifying an application including locating, retrieving, reviewing, and copying any material requested. The College will provide an estimate of any charge on request or if it appears that the work will be onerous, or the information sought is extensive. If the College is unable to provide access to that information, in most cases, written notice will be provided explaining the reasons for refusal.

### 3.3. Consent and Restrictions on Rights of Access to the Personal Information of Students

The College respects every parent/guardian right to make decisions concerning their child's education.

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

Parents/guardians may seek access to personal information held by the College about them or their child by contacting the College's Privacy Officer. However, there will be occasions when access will be denied. Such occasions include where the request for, or release of, the information:

- would have an unreasonable impact on the privacy of others;
- would pose a serious threat to the life, health, or safety of any individual or to public health or public safety;
- is frivolous or vexatious;
- where the release may result in a breach of the College's duty of care to the student.

The College may, at its discretion, on the request of a student grant that student access to information held by the College about them or allow a student to give or withhold consent to the use of their personal information, independently of their parents/guardians. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warrant.

### 3.4. Third Parties

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

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

## 4. Data Breaches

In the event of a data breach, the School's Data Breach Response Process will be followed (as explained in the Responsible Use of ICT Policy).

## 5. Complaints Resolution

Any complaints about the way the College manages personal information, are to be directed to the College in the first instance. The College's Privacy Officer will:

- listen to concerns and grievances regarding the handling of personal information.
- discuss ways in which the situation can be remedied.
- devise an action plan to resolve the complaint and improve information handling procedures (if appropriate).

## 6. Contact Information

Access to any personal information that is held, or requests for further information regarding the manner in which the College manages the personal information it holds are to be directed to the Privacy Officer, as listed below.

### *Privacy Officer*

Overnewton Anglican Community College

Telephone: + 61 3 9334 0000

Email: [privacy.officer@overnewton.vic.edu.au](mailto:privacy.officer@overnewton.vic.edu.au)

# Policy Status and Review

The Principal is responsible for reviewing and updating the Community Code of Conduct for Adults at least every two years. The review will include input from the Deputy Principal Head of Campus and the Director of Wellbeing. The Risk Management Committee will provide final approval of the policy.

Document Details	
Date Created	2013
Date Reviewed	September 2024
Next Review Date	September 2026
Policy Owner	Principal
Approved By	Risk Management Committee

Version Control				
Version	Date	Description	Reviewed by/Date	Approved by/Date
1	2013	Policy Created	2013	2013
2 & 3	2016 & 2019	Policy Review and Update	2021	2021
4	June 2024	Policy Review and Update Included Child Safety and Policy Definitions	PPWG & SME - June 2024	
5	September 2024	Reviewed by RMC	24 <sup>th</sup> September 2024	RMC - September 2024

# Appendix A

## Process 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 (e.g. 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**

When developing or reviewing a project, consider the need for a privacy impact assessment (PIA). A PIA identifies how 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