



<i>Name of policy</i>	PRIVACY POLICY
<i>Policy context</i>	<p>Aquinas College is a residential community of adult learners that draws on the richness of the Catholic intellectual tradition and embraces the best in contemporary approaches to tertiary education and student residential care. The College seeks to be a safe, just, compassionate, responsive and inclusive place for all its residents and its employees.</p> <p>The mutual obligations of its members are defined by Catholic social teaching and all relevant laws and regulatory frameworks of the State of South Australia and the Commonwealth of Australia. Entrusted to the care of the Marist Brothers (Province of Australia), Aquinas College aspires to be an educative community of faith and justice influenced by Marist spirituality and shaped by Marist educational principles.</p> <p>The College is governed by a Council appointed by the Archbishop of Adelaide. Its policies and protocols complement those of the Archdiocese of Adelaide and the Marist Association of Saint Marcellin. For any matter where there is no specific College policy or protocol, the custom and practice of the Archdiocese apply.</p> <p>This policy document operates within this global context and in conjunction with other College policies named below.</p>
<i>Purpose and scope</i>	<p>The purpose of this policy is to ensure that in the course of Aquinas College's activities, it manages and protect personal information in accordance with the Privacy Act (1988, as amended) and the Australian Privacy Principles (APPs). The policy outlines the circumstances in which the College obtains personal information, how it uses that information, how it manages requests to access and/or change that information, and how it deals with data breaches.</p> <p>The policy applies to all present and past staff (full-time, part-time and student staff), visiting clergy and religious, volunteers and external contractors of Aquinas College and its related bodies.</p>

Currency	Commencement date: August 2018 (updated) Intended review date: June 2022 <i>(The policy remains operative until a review takes place and/or it is updated or terminated.)</i>
Approval Authority	College Council
Responsible officer(s)	Rector
Related policies and protocols	Social Media Policy IT and Internet Usage Policy Staff Appointment and Induction Policy Grievance and Complaint Resolution Policy

1.0 Policy Statement

- 1.1. Aquinas College fosters a culture and regimen of privacy which protects personal information concerning its present and past residents and staff, as well as any information it has that concerns other people who are or have had dealings with the College.
- 1.2. The College complies with the APPs and takes all reasonable steps to ensure the safe keeping of private information and to its being accurate, up to date and complete.
- 1.3. The College collects personal information relevant to the residency, employment and/or business of people with or at the College.

2. Procedures

2.1. *Types of information collected*

Depending on the circumstances, the College may collect personal information from or about individuals relating to their being a student, contractor, volunteer, stakeholder, present or potential employee, governor, or in some other capacity.

In the course of providing services the College may collect and hold:

- *personal information* including names, addresses, and other contact details; visual images; dates of birth; and financial information;
- *sensitive information* including government identifiers (such as Tax File Number [TFN]), nationality, country of birth, professional memberships, family court orders and criminal records;
- *health information* (particularly in relation to prospective staff and student records) including medical records, disabilities, immunisation details and psychological reports.

As part of our recruitment processes for employees, contractors and volunteers, the College may collect and hold:

- *personal information* including names, addresses and other contact details, dates of birth, financial information, citizenship, employment references, regulatory accreditation, media, directorships, property ownership, visual images, and driver's licence information.

- *sensitive information* including government identifiers (such as TFN), nationality, country of birth, professional memberships, family court orders and criminal records.
- *health information* (particularly in relation to prospective staff and student records) including medical records, disabilities, immunisation details and psychological reports.

2.2 **Methods of collecting information**

The collection of personal information depends on the circumstances for which Aquinas College is collecting it. Generally, the College seeks consent from the individual in writing or by action before it collects sensitive information. If it is reasonable and practical to do so, the College collects personal information directly from the individual.

2.2.1 *Solicited Information*

Aquinas College attempts, where possible, to standardise the collection of personal information by using specifically designed forms (e.g. Application Forms). Given the nature of the College's operations, however, personal information is also received by email, letters, notes, via the College website, over the telephone, in face-to-face meetings and through financial transactions.

The College may also collect personal information from other people or entities (e.g. a third-party administrator, referees for prospective employees) or independent sources. However, it will only do so where it is not reasonable or practical to collect the personal information from the individual directly.

2.2.2 *Information collected from the College website*

The College may collect information based on how individuals use or access our website. The College uses 'cookies' and other data collection methods to collect information on website activity such as the number of visitors, the number of pages viewed and the internet advertisements which bring visitors to our website. This information is collected to analyse and improve the website, marketing campaigns, College events, and to record statistics on web traffic.

2.2.3 *Information collection from the LAN*

The College may collect information from use of its local area network. The College reserves the right to view with justifiable reason emails sent or received by an employee or agent of the College. The College collects data regarding internet usage on the College network in order to generate data on usage and access of devices, improve the efficiency of the network, identify any activity that is against the IT Usage Policy, provide a safe online environment, and generally safeguard its residents and staff and ensure the good order of the College.

2.2.4 *Unsolicited information*

Aquinas College may be provided with personal information without having sought it through normal means of collection. This unsolicited information can be often collected by:

- misdirected postal mail – letters, notes, documents
- misdirected electronic mail – emails, electronic messages
- employment expressions of interest that are not in response to an advertised vacancy
- additional information provided to the College which was not requested.

Unsolicited information obtained by Aquinas College will only be held, used and or disclosed if it is considered as personal information that could have been collected by normal means. If that unsolicited information could not have been collected by normal means then it will be destroyed, permanently deleted or de-identified as appropriate.

2.2.5 *Collection of sensitive information*

The College only collects sensitive information if it is:

- reasonably necessary for one or more of these functions or activities, and there is consent
- necessary to lessen or prevent a serious threat to life, health or safety
- another permitted general situation
- another permitted health situation.

2.3 *Use of personal information*

Aquinas College only uses personal information that is reasonably necessary for one or more of its functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected by the individual, or for an activity or purpose to which the individual has consented.

The College’s primary uses of personal information include, but are not limited to:

- providing accommodation and residency services
- providing education and support of students in their studies
- extra-curricular and health services
- satisfying its legal obligations
- the employment of staff and the engagement of volunteers
- helping it to improve our day-to-day operations including training of staff
- keeping parents and care-givers informed and seeking information from them through correspondence, invitations, newsletters, college magazine and other publications
- marketing, promotional and fundraising activities
- supporting the activities of the College groups such as among its alumni
- supporting community-based causes and activities, charities and other causes in connection with the College’s functions or activities
- systems development
- developing new programs and services
- undertaking planning, research and statistical analysis
- College administration including for insurance purposes

Consent to include visual images of students, alumni, staff, volunteers, visiting clergy and governors in College newsletters and other publications, on the College website, in publications of corporate entities directly associated with the College (the Marist

Brothers and the Archdiocese of Adelaide), and in College advertising and publicity, is presumed. Any persons who do not wish their images to be used in one or more of these media, is required to notify the Rector.

The secondary purposes include but are not limited to

- sharing of information with other entities for health or legal reasons
- sharing of information with other entities because it is necessary to do so
- disclosing information about an individual to overseas recipients only when it is necessary, for example, to facilitate a visa or exchange programme, and only with the consent of the individual.

2.4 ***Storage and security of personal information***

Aquinas College stores personal information in a variety of formats including, but not limited to:

- electronic databases
- hard copy files
- personal devices, including laptop computers
- third party storage providers such as cloud storage facilities

The College takes all reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure. These steps include, but are not limited to:

- restricting access and user privilege of information by staff depending on their role and responsibilities.
- requiring staff not share personal passwords
- requiring staff to change passwords regularly
- storing hard copy files in lockable filing cabinets in lockable rooms, with staff access subject to user privilege.
- securing access to Aquinas College's premises
- ensuring the College's IT and cyber security systems, policies and procedures are implemented and up to date
- requiring staff to comply with internal policies and procedures when handling the information
- undertaking due diligence with respect to third party service providers who may have access to personal information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the APPs
- destroying, disposing of, deleting or de-identifying personal information that is no longer needed, has no justifiable archival value or purpose, or is not required to be retained by any other laws.

Aquinas College's website may contain links to other third-party websites outside of the College. Aquinas College is not responsible for the information stored, accessed, used or disclosed on such websites or for their privacy policies and procedures.

2.5 ***Responding to data breaches***

Aquinas College takes appropriate and prompt action if it has reasonable grounds to believe that a data breach may have, or is suspected to have occurred. Depending on the type of data breach, this may include a review of internal security procedures,

taking remedial internal action, or notifying affected individuals. If the College is unable to notify individuals directly, it will publish a statement on the Aquinas website.

If a data breach occurs which is notifiable under the Notifiable Data Breach Scheme, then:

- every reasonable effort is made immediately to contact any or all persons whose data may have been lost or stolen;
- the Office of the Australian Information Commissioner is notified using the online form available on its website: www.oaic.gov.au.

2.6 Disclosure of personal information

Personal information may be disclosed to government agencies, related entities and other recipients from time to time, if the individual has given consent or would reasonably expect the personal information to be disclosed in that manner.

Aquinas College may disclose personal information without consent or in a manner which an individual would reasonably expect if:

- the College is required to do so by law.
- the disclosure would lessen or prevent a serious threat to the life, health or safety of an individual or to public safety.
- another permitted general situation applies.
- disclosure is reasonably necessary for a law enforcement related activity.
- another permitted health situation exists.

Personal information about an individual may be disclosed to an overseas organisation in the course of providing services, for example when storing information with a “cloud service provider” which stores data outside of Australia. The College takes all reasonable steps not to disclose an individual’s personal information to overseas recipients unless it

- has the individual’s consent (which may be implied);
- is satisfied that the overseas recipient is compliant with the APPs, or a similar privacy regime;
- it is of the opinion that the disclosure would lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
- is taking appropriate action in relation to suspected unlawful activity or serious misconduct.

2.7 The quality of personal information

Aquinas College takes all reasonable steps to ensure the personal information it holds, uses and discloses is accurate, complete and up-to-date, including at the time of using or disclosing the information. If the College becomes aware that personal information is incorrect or out of date, it takes reasonable steps to rectify the incorrect or out of date information.

2.8 Access and correction of personal information

Individuals may submit a request to Aquinas College to access the personal information that the College holds, or request that it amend this information. Upon receiving such a request, the College takes steps to verify the individual’s identity

before granting access or correcting the information. If the College rejects the request, the applicant will be notified accordingly. Where appropriate, the College provides the reason/s for its decision. If the rejection relates to a request to amend personal information, an individual may make a statement about the requested change and this will be attached to their file.

2.9 **Complaints**

A person can lodge a complaint about how Aquinas College manages personal information by notifying the College, preferably without delay. The College responds to the complaint within a reasonable time (usually no longer than 30 days) and may seek further information in order to provide a full and complete response.

The College does not normally charge a fee for the handling of complaints.

If the complainant is not satisfied with the response, he or she may refer the complaint to the OAIC. A complaint can be made using the OAIC online Privacy Complaint form or by mail or email. A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

2.10 **How to contact the College**

Aquinas College can be contacted about this Privacy Policy or about personal information generally, by:

- Email: privacy@aquinas.edu.au
- Telephone +61 8 8335 5000
- Writing to the Privacy Officer at 1 Palmer Place, North Adelaide 5006.

If a person makes contact anonymously or by using a pseudonym, the College will do its best to respond but it may not be able to provide that person with the information or assistance they might otherwise receive if their identity is known.

2.11 **Updates**

This Privacy Policy is subject to change at any time. The latest version is posted on the Aquinas College website: www.aquinas.edu.au.

Appendix A Glossary & Definitions

Australian Privacy Principles	13 principles active from 12 March 2014 through the Privacy Amendment (Enhancing Privacy Protection Act) 2012 and which apply to all organisations in Australia.
Personal information	<p>Information or an opinion whether true or not and whether recorded in a material form or not, about a person whose identity is apparent or can reasonably be ascertained.</p> <p>In this Privacy Policy, in addition to generic 'personal information', also included are 'health information' and 'sensitive information'</p> <p>Health information is a subset of personal information that is generally afforded a higher level of privacy protection. Health information relates to the health or disability of an individual, the provision of health services to the individual or the individual's expressed wishes about the provision of health services.</p> <p>Sensitive Information is another subset of personal information that is generally afforded a higher level of privacy protection. It includes information about racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association or trade union, sexual preferences or practices, criminal record and some types of biometric information.</p>
OAIC	Office of the Australian Information Commissioner.
Notifiable Data Breach Scheme	A scheme pursuant to the Privacy Act (1988) which has been operative in Australia since February 2018, and enacted in the Privacy Amendment (Notifiable Data Breaches) Act 2017. Further information available at www.oaic.gov.au .