

Privacy Policy

1. Purpose

The purpose of this policy is to ensure that in the course of St Michael's College activities personal information is protected in accordance with the Privacy Act 1988 (Cth) (Privacy Act) and the 13 Australian Privacy Principles (APPs).

2. Scope

This policy outlines the circumstances in which personal information is obtained, how that information is used and how requests to access and/or change that information is managed. This policy applies to all staff, volunteers and contractors of St Michael's College and its related bodies.

3. Definition

What is personal information and how is it collected?

Personal information is information or an opinion about an individual from which they can be reasonably identified. Depending on the circumstances, the College may collect personal information from the individual in their capacity as a student, contractor, volunteer, stakeholder, job applicant or in some other capacity.

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

- **Personal Information** including names, addresses and other contact details; dates of birth; and financial 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 customer records) including medical records, disabilities, immunisation details and psychological reports.

As part of the 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 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.

Generally, the College will seek consent from the individual, in writing, prior to collecting sensitive information (including health information).

4. Statement

It is the policy of St Michael's College regarding the following matters:

4.1 Collection of personal information

The collection of personal information depends on the circumstances in which St Michael's College is collecting it. If it is reasonable and practical to do so, personal information is collected directly from the individual.

4.2 Solicited Information

St Michael's College has, where possible, attempted to standardise the collection of personal information by using specifically designed forms (e.g. Enrolment Application Forms). However, given the nature of its operations, the College often receives personal information by emails, letters, notes, website, telephone, through face-to-face meetings and through financial transactions.

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

4.3 Information collected from our website

Information based on how individuals use the College's website may be recorded. "Cookies" and other data collection methods may be used 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 our website, marketing campaigns and to record statistics on web traffic and is not used to personally identify individuals.

4.4 Unsolicited information

St Michael's College may be provided with personal information without having sought it through normal means of collection. This is known as "unsolicited information" and is often collected by:

- Misdirected postal mail – Letters, Notes, Documents;
- Misdirected electronic mail – Emails, electronic messages;
- Employment applications received that are not in response to an advertised vacancy;
- Additional information provided which was not requested.

Unsolicited information obtained by St Michael's 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 it will be destroyed, permanently deleted or personal information de-identified the as appropriate.

4.5 Collection and use of sensitive information

The College will only collect sensitive information if it is:

- reasonably necessary for one or more of these functions or activities, and if the individual's consent has been obtained;
- necessary to lessen or prevent a serious threat to life, health or safety;
- another permitted general situation;
- another permitted health situation.

The College may share sensitive information to other entities in its company group, but only if necessary to provide products or services.

4.6 How do we use personal information?

St Michael's 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.

Primary uses of personal information include, but are not limited to:

- providing education, pastoral care, extra-curricular and health services;
- satisfying our legal obligations including our duty of care and child protection obligations;
- keeping parents informed as to school community matters through correspondence, newsletters and magazines;
- marketing, promotional and fundraising activities;
- supporting the activities of school associations such as Alumni/Old Scholars;
- supporting community based causes and activities, charities and other causes in connection with the St Michael's College functions or activities;
- improving our day-to-day operations including staff training;
- systems development; developing new programs and services; undertaking planning, research and statistical analysis;
- College administration including for insurance purposes;
- the employment of staff; and
- the engagement of volunteers.

The College will only use or disclose sensitive or health information for a secondary purpose if the individual reasonably expects for this information to be disclosed and if the secondary purpose is directly related to the primary purpose.

The College may share personal information to related bodies corporate, but only if necessary to provide its services.

The College may disclose information about an individual to overseas recipients only when it is necessary, for example to facilitate a student exchange program. The College will not however send information about an individual outside of Australia without their consent.

4.7 Storage and Security of Personal Information

St Michael's College stores personal information in a variety of formats including, but not limited to:

- databases;
- hard copy files;
- personal devices, including laptop computers;
- third party storage providers such as cloud storage facilities;
- paper based files.

St Michael's College takes all reasonable steps to protect the personal information held 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;
- Ensuring staff do not share personal passwords;
- Ensuring hard copy files are stored in lockable filing cabinets in lockable rooms. Staff access is subject to user privilege;
- Ensuring access to St Michael's College premises are secured at all times;
- Ensuring IT and cyber security systems, policies and procedures are implemented and up to date;
- Ensuring staff 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 Australian Privacy Principles or a similar privacy regime.
- The destruction, deletion or de-identification of personal information held that is no longer needed, or required to be retained by any other laws.

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

4.8 Responding to data breaches

St Michael's College will take appropriate and prompt action if there are 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, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC).

If the College is unable to notify individuals, a statement will be published on the College website and reasonable steps will be taken to publicise the contents of this statement.

4.9 Disclosure of personal information

Personal information is used for the purposes for which it was given to St Michael's College or for purposes which are directly related to one or more of its functions or activities. 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.

St Michael's College may disclose personal information without consent or in a manner which an individual would reasonably expect if:

- they are required to do so by law;
- the disclosure will 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.

4.10 Disclosure of your personal information to overseas recipients

Personal information about an individual may be disclosed to an overseas organisation in the course of providing our services, for example when storing information with a "cloud service provider" which stores data outside of Australia. The College will, however, take all reasonable steps not to disclose an individual's personal information to overseas recipients unless:

- the individual's consent has been given (which may be implied);
- the College is satisfied that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime;
- the College forms the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
- the College are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

4.11 The quality of personal information

The College takes all reasonable steps to ensure the personal information held, used and disclosed is accurate, complete and up-to-date, including at the time of using or disclosing the information.

If St Michael's College becomes aware that the personal information is incorrect or out of date, it will take reasonable steps to rectify the incorrect or out of date information.

4.12 Access and correction of personal information

Individuals may submit a request to the College to access the personal information held, or request that the College change the personal information. Upon receiving such a request, the College will take steps to verify the individual's identity before granting access or correcting the information.

If the College rejects the request, the individual will be notified accordingly. Where appropriate, the College will provide the reason/s for the decision. If the rejection relates to a request to change personal information, an individual may make a statement about the requested change and the College will attach this to their record.

4.13 Complaints

An individual can make a complaint about how St Michael's College manages personal information by notifying the College in writing as soon as possible. The College will respond to the complaint within a reasonable time (usually no longer than 14 days) and will seek further information in order to provide a full and complete response.

St Michael's College does not charge a fee for the handling of complaints.

If the individual is not satisfied with the College's response, they may refer the complaint to the OAIC. A complaint can be made using the OAIC online [Privacy Complaint form](#) or by mail, fax or email. A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

4.14 How to contact us

St Michael's College can be contacted about this Privacy Policy or about personal information generally, by:

- Emailing pa@smc.sa.edu.au
- Calling 08 8356 5966
- Writing to the Privacy Officer at St Michael's College, 15 Mitton Avenue, Henley Beach SA 5022 or by facsimile at 08 8356 1092

If practical, an individual may contact the College anonymously (i.e. without identification) or by using a pseudonym. However, if the individual chooses not to identify themselves, the College may not be able to provide the information or assistance that might otherwise be provided and if it is not practical to do so.

4.15 Changes to our privacy and information handling practices

This Privacy Policy is subject to change at any time.

This Privacy Policy was last reviewed: **2 May 2018**

5. Related policies, procedures and support documents

This Policy is to be read in conjunction with the following documents:

- Privacy Act 1988
- SACCS Privacy Policy (2014)

6. Revision Record

Document Title	Privacy
Document Type	Policy
Document Date	April 2018
Policy Owner	Office of the Principal
Approval Authority	Principal
Risk Rating	Extreme
Review Date	April 2019
Revision History	2017, 2018

7. Risk Matrix

Likelihood	Consequences				
	1. Insignificant	2. Minor	3. Moderate	4. Major	5. Catastrophic
A. (Almost Certain)	M	M	H	E	E
B. (Likely)	L	M	H	E	E
C. (Possible)	L	M	M	H	E
D. (Unlikely)	L	L	M	M	H
E. (Rare)	L	L	L	M	H