



PRIVACY POLICY

RATIONALE

St Kevin's College is a Catholic school in the Edmund Rice tradition. A member of the Edmund Rice Education Australia (EREA) network of schools, the College is committed to protecting the privacy of all stakeholders including staff.

PURPOSE

The Privacy Act 1988 (Cth) requires St Kevin's College, as a member entity of EREA, to handle any personal information (including sensitive information) we collect about individuals in accordance with the thirteen Australian Privacy Principles (APP's).

Under Principle 1 of the APP's, St Kevin's College is required to develop a Privacy Policy that sets out how we manage personal information in addition to making the Policy available on our public website.

The St Kevin's College Privacy Policy has been established in accordance with EREA's Charter and is underpinned by the core values of EREA and St Kevin's College.

POLICY STATEMENT

St Kevin's College will have a Privacy Policy that conforms with the thirteen Australian Privacy Principles found in the Privacy Act 1988 (Cth) and with the Privacy Amendment (Notifiable Data Breaches) Act 2017(Cth). The Policy will also conform to state-based legislation in relation to health records.

COLLECTION OF PERSONAL INFORMATION

Personal information is information or an opinion about an individual from which they can be reasonably identified. The College may collect personal information from an individual in their capacity as a current or prospective student, contractor, volunteer, job applicant, employee, alumni, visitor or others who come into contact with the College.

If it is reasonable and practical to do so, the College will collect personal information directly from the individual.

The kinds of personal information we collect is largely dependent upon whose information we are collecting and why we are collecting it, however in general terms, the College may collect:

- Personal Information including names, addresses and other contact details, dates of birth, next of kin details, financial information, photographic images and attendance records.
- Sensitive Information (particularly in relation to student and parent records) including religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional or union membership, family court orders and criminal records.
- Health Information (particularly in relation to student and parent records) including medical records, disabilities, immunisation details, individual health care.

If the personal information is sensitive information (including health information), then the College will obtain the individual's consent (which may be implied) to the collection.

It is noted that employee records are not covered by the Australian Privacy Principles or the Health Privacy Principles where they relate to current or former employment relations between the College and the employee.

HOW WE COLLECT PERSONAL INFORMATION

The College has, where possible, attempted to standardise the collection of personal information by using specifically designed forms to ensure that only the information required to provide our services is collected.

However, the College may also receive personal information necessary to effectively deliver its services or meet its legislative obligations and duty of care via email, letters, notes, via our website, over the telephone, in face-to-face meetings, through financial transactions, through the use of "cookies" for web browsing and through surveillance activities such as the use of CCTV security cameras or email monitoring.

The College may also collect personal information from other sources (e.g. a third-party administrator, referees for prospective employees etc.). Personal information will only be collected from third parties where it is not reasonable and practical to collect the personal information from the individual directly.

UNSOLICITED INFORMATION

The College may receive personal information about an individual in circumstances where we have taken no active step to collect the information. This is known as unsolicited personal information.

Examples of unsolicited personal information the College collects include:

- a note from a student or their parents/carers
- misdirected mail
- petitions including names and addresses
- job applications not in response to an advertised job vacancy
- a promotional flyer/leaflet promoting an individual's business containing an email address or mobile phone number
- personal information that is provided to us that is additional to the information solicited by us (for example if an individual completes an application or information request and provides additional personal information that was not requested).

If the College receives unsolicited information, we must determine whether it is necessary for one or more of our activities or functions. If it is not necessary, we must destroy or de-identify it.

If it is necessary, we must treat it as we would treat any solicited information we have collected.

USE OF PERSONAL INFORMATION

The College only uses personal information that is reasonably necessary for one or more of our 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 an individual has consented.

The College's 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 College community matters through correspondence, newsletters and magazines
- Marketing, promotional and fundraising activities
- Supporting the activities of College associations
- Supporting community-based causes and activities, charities and other causes in connection with the College's functions or activities
- Helping us to improve our day-to-day operations including training our staff

- Systems development; developing new programs and services; undertaking planning, research and statistical analysis
- College administration including for insurance purposes the employment of staff and engagement of volunteers.

We will only use or disclose sensitive or health information for a secondary purpose if an individual would reasonably expect us to use or disclose the information and the secondary purpose is directly related to the primary purpose. We may share personal information with related bodies corporate, but only if necessary for us to provide our services.

STORAGE AND SECURITY OF PERSONAL INFORMATION

Personal information is stored on College servers and through the use of third party cloud services. The College is committed to ensuring that cloud based services comply with legislative obligations and address the College's privacy and security requirements.

RESPONDING TO DATA BREACHES

The College maintains procedures for responding to data breaches, including initial containment, formal investigation and the formation of a data breach response team.

The College will take appropriate, prompt action if we have 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 our internal security procedures, taking remedial internal action, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC). If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

DISCLOSURE OF PERSONAL INFORMATION

Personal information is used for the purposes for which it was given to the College, or for purposes which are directly related to one or more of our functions or activities. Personal information may be disclosed to government agencies, other parents, other schools, employees, recipients of College publications, visiting teachers, counsellors and coaches, our service providers, agents, contractors, business partners, 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.

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

- We 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
- Disclosure is reasonably necessary for a law enforcement related activity
- Another permitted general situation applies
- Another permitted health situation exists.

OVERSEAS DISCLOSURE

The College may disclose information about an individual to overseas recipients only when it is necessary. Examples of when the College may disclose personal information to an overseas recipient include:

- publishing unsecured personal information using a cloud-based computer storage service with servers based outside Australia
- sending emails or hard copy documents containing personal information to an overseas recipient, especially when organising overseas trips or facilitating a student exchange
- discussing personal information at an overseas meeting or with an overseas recipient over the phone and making a record of it
- publishing personal information on the internet (for example on social media sites such as Facebook or Twitter) that is accessible by overseas recipients
- using online applications (apps or other services) provided by an overseas third party service provider for services such as email, instant messaging, learning and assessment tools
- providing personal information to an overseas contractor or service provider including for excursions.

Where the College discloses personal information to an overseas recipient, the College is legally accountable if the overseas recipient mishandles the personal information, unless one of the following applies:

- the overseas recipient is subject to the laws of a country, or a binding scheme, that we reasonably believe to be substantially similar to the protections afforded to personal information under the APPs and an individual can access mechanisms to enforce the protections of the law or binding scheme
- we have the individual's consent, after expressly informing them in a statement of the potential consequences of providing consent
- a Permitted General Situation or a Permitted Health Situation exists (refer to OAIC Guidance Materials section for more information).

PERSONAL INFORMATION OF STUDENTS

The Privacy Act does not differentiate between adults and children and does not specify an age after which individuals can make their own decisions with respect to their personal information.

The College will take a 'common-sense' approach to dealing with a student's personal information and generally will refer any requests for personal information to a student's parents/carers. We will treat notices provided to parents/carers as notices provided to students and we will treat consents provided by parents/carers as consents provided by a student.

In seeking to respect the rights of children under the Privacy Act and recognising that in certain circumstances (especially when dealing with older students and when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. We also acknowledge that there may be occasions where a student may give or withhold consent with respect to the use of their personal information independently from their parents/carers.

There may also be occasions where parents/carers are denied access to information with respect to their children, because to provide such information would have an unreasonable impact on the privacy of others, or result in a breach of the College's duty of care to the student.

QUALITY OF PERSONAL INFORMATION

The College must have practices, procedures and systems in place to ensure that the personal information it collects, uses, holds and/or discloses is accurate, up-to-date, complete and relevant. The rationale behind this requirement is to prevent situations where the College may use or disclose, inaccurate, incomplete or out-of-date personal information.

The College has established and effectively implemented practices, procedures and systems to ensure that the personal information the College collects, uses, holds and/or discloses is accurate, up-to-date, complete and relevant at the time the information is collected and again when the information is used or disclosed.

ACCESS TO PERSONAL INFORMATION

Individuals have the right of access to any personal information we hold about them. There are some limited exceptions to this right of access including where access would:

- be unlawful
- pose a serious threat to the life or health of another individual
- unreasonably impact on the privacy of others

- require us to disclose evaluative information in connection with a commercially sensitive matter
- adversely impact an internal investigation into unlawful activities
- be considered frivolous or vexatious
- reveal our intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations
- involves legally privileged information during legal proceedings.

Where a request for access to personal information is made the College will respond within a reasonable time. If access is denied the College will provide:

- written notice for the reasons for refusal (except where it would be unreasonable to do so)
- the mechanisms available to complain about the refusal.

The Privacy Act allows the College to impose a charge that is designed to cover costs, however this charge must not be excessive and the College must disclose this charge to the individual upfront. Where access can be given, the College must endeavour to provide it in a manner that is as prompt, uncomplicated and as inexpensive as possible.

COMPLAINTS

The College takes all complaints seriously. Privacy complaints can be made to the College's Privacy Officer and will be dealt with on a similar basis to any other inquiries and complaints we receive. Inquiries and complaints can arise verbally or in writing.

CONTACT US

Governance Advisor at St Kevin's College is the College Privacy Officer. The College Privacy Officer can be contacted at:

privacy@stkevins.vic.edu.au

(03) 9822 0911

31 Moonga Rd, Toorak VIC 3142

Director of Risk and Compliance for Edmund Rice Education Australia (EREA) is the Privacy Officer for all EREA. The EREA Privacy Officer can be contacted at:

complaints@erea.edu.au

(03) 9426 3200

PO Box 91, Richmond VIC 3121

RELATED INFORMATION

Privacy Act 1988 (Cth)

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Australian Privacy Principles (APP)

Health Records Act (Vic)