PRIVACY POLICY

CATEGORY

Governance

BACKGROUND

The purpose of this policy is to ensure that in the course of Penrhos College's activities, we manage and protect personal information in accordance with the Privacy Act 1988 (Cth) (**Privacy Act**), and the 13 Australian Privacy Principles (APPs).

SCOPE OF POLICY

This policy outlines the circumstances in which we obtain personal information, how we use that information and how we manage requests to access and/or change that information.

This policy applies to all staff, volunteers and contractors of Penrhos College and its related bodies.

Job applicants and staff members:
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 College's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the College and employee.

Duty of Care
In the case of students, any conflict between the Privacy Act requirements and Duty of Care obligations under the Education Act, Duty of Care takes precedence if the student is considered at risk of harm or harm to others. These decisions are made on a case by case basis and in consultation with all or some of the following staff members: Principal, Dean of Pastoral Care, Head of Junior School, Head of Boarding, Counsellors, School Nurse. Decisions are based on the premise that 'foreseeable and preventable risk' to the student is minimised.

What is personal information and how do we collect it?

Personal information is information or an opinion about an individual from which they can be reasonably identified. Depending on the circumstances, we 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 we may collect and hold:

- **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 our recruitment processes for employees, contractors and volunteers, we 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, we will seek consent from the individual in writing before we collect their sensitive information (including health information).

Collection of personal information

The collection of personal information depends on the circumstances in which Penrhos College is collecting it. If it is reasonable and practical to do so, we collect personal information directly from the individual.

Solicited Information

Penrhos College has, where possible, attempted to standardise the collection of personal information by using specifically designed forms (e.g. our Application Forms). However, given the nature of our operations we often also receive personal information by email, letters, notes, via our website, over the telephone, in face-to-face meetings and through financial transactions.

We 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.

Information collected from our website

We may collect information based on how individuals use our website. "Cookies" may be used 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 our website, marketing campaigns and to record statistics on web traffic. We do not use this information to personally identify individuals.

Unsolicited information

Penrhos College may be provided with personal information without having sought it through our 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 sent to us that are not in response to an advertised vacancy
- Additional information provided to us which was not requested.

Unsolicited information obtained by the 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 we will destroy, permanently delete or de-identify the personal information as appropriate.

Collection and use of sensitive information

We only collect sensitive information if it is:

- reasonably necessary for one or more of these functions or activities, and we have the individuals consent
- necessary to lessen or prevent a serious threat to life, health or safety
- another permitted general situation
- another permitted health situation

How do we use personal information?

Penrhos 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 the individual has consented.

Our 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 the Penrhos College Alumni
- supporting the activities of the College Foundation
- supporting community-based causes and activities, charities and other causes in connection with the School'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
- school administration including for insurance purposes
- the employment of staff
- the engagement of volunteers.

We will only use or disclose sensitive or health information for a secondary purpose if you 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 to related organisations, but only if necessary for us to provide our 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.

Storage and Security of Personal Information

Penrhos College stores Personal Information in a variety of formats including, but not limited to:

- databases
- personal devices, including notebook computers
- third party storage providers such as cloud storage facilities
- paper-based files.

We take all reasonable steps to protect the personal information we hold 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 paper-based files are stored in lockable filing cabinets in lockable rooms. Staff access is subject to user privilege.
- Ensuring access to the College's premises are secured at all times.
- Ensuring our 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 we hold that is no longer needed or required to be retained by any other laws.

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

Responding to data breaches

Penrhos 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 Penrhos, or for purposes which are directly related to one or more of our 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.

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

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.

We will however take all reasonable steps not to disclose an individual's personal information to overseas recipients unless:

- we have the individual's consent (which may be implied);
- we have satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime;
- we form 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
- we are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

The quality of personal information

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up-to-date, including at the time of using or disclosing the information.

If Penrhos becomes aware that the Personal Information is incorrect or out of date, we will take reasonable steps to rectify the incorrect or out of date information.

Access and correction of personal information

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

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

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. This would normally be done only when the maturity of the student and/or the student's personal circumstances so warranted.

Complaints

An individual can make a complaint about how Penrhos College manages personal information by notifying us in writing as soon as possible. We will respond to the complaint within a reasonable time (usually no longer than 30 days) and we may seek further information in order to provide a full and complete response.

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

If the individual is not satisfied with our 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.

Note: A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted.

How to contact us

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

- Emailing [email address privacy@penrhos.wa.edu.au
- Calling 08 9368 9500
- Writing to our Privacy Officer at Locked Bag 690, COMO 6952 or by facsimile at 08 9368 9677.

If practical, you can contact us anonymously (i.e. without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

Changes to our privacy and information handling practices

This Privacy Policy is subject to change at any time. Please check our Privacy Policy on our website (www.penrhos.wa.edu.au) regularly for any changes.

DEFINITIONS:

Sensitive information means:

(a) Information or an opinion about an individual's:

- racial or ethnic origin; or
- political opinions; or
- membership of a political association; or
- religious beliefs or affiliations; or
- philosophical beliefs; or
- membership of a professional or trade association; or
- membership of a trade union; or
- sexual preferences or practices; or
- criminal record;

That is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

Health information means:

(a) Information or an opinion about:

- the health or a disability (at any time) of an individual; or
- an individual's expressed wishes about the future provision of health services to him or her; or
- a health service provided, or to be provided, to an individual;

That is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual

Eligible Data Breach means:

(a) unauthorised access or disclosure, or loss of information where unauthorised access or disclosure is likely; and

(b) a reasonable person would conclude that the access or disclosure would likely result in serious harm to the individuals to whom the information relates.

ASSOCIATED POLICIES AND PROCEDURES

Duty of Care Policy
Communications Policy
Records Management Policy

LAST UPDATE: MARCH 2018