PRIVACY POLICY

This policy was last updated June 2024
To be reviewed in June 2026

Scope of Policy and Source of Obligation

Donvale Christian College (the College) values privacy and is committed to protecting information that it collects. The College manages and protects personal information in accordance with the Privacy Act 1988 (Cth) (Privacy Act), the 13 Australian Privacy Principles (APPs) and the requirements of Health Records Act (Vic).

Scope of Policy

This policy outlines the circumstances in which the College obtains personal information, how its uses and discloses that information and how it manages requests to access and/or change that information.

What is personal information and how does the College collect it?

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, job applicant, alumni, visitor or others that come into contact with the College.

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

- **Personal Information** including names, addresses and other contact details; date of birth; next of kin details; photographic images; attendance records and financial information.
- **Sensitive Information** including government identifiers, religious beliefs, nationality, country of birth, professional memberships and family court orders.
- **Health Information** including medical records, disabilities, immunisation details, counselling notes 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, salary and financial information, citizenship, employment references, regulatory accreditation, media, and licence information.
- **Sensitive Information** including government identifiers (such as TFN), nationality, country of birth, professional memberships and criminal records.

- **Health Information** including health information (including allergies and medical certificates) and disabilities.

Generally, the College will seek consent from the individual in writing before it collects sensitive information (including health information).

Employee records are not covered by the APPs or the Health Privacy Principles where they relate to current or former employment relations between the College and the employee.

This exemption does not apply to:

- employees that are employed through a related corporation.
- employee records that are provided to a third party such as an educational authority, external training provider, recruiter or payroll service.
- personal information collected from prospective employees who are subsequently not employed by the College, such as unsuccessful job applicants or individuals who send in unsolicited applications.

Collection of Employee Information

Employment information is exempt from the Privacy Act after it has been collected, but the collection of the information from employees, is not exempt. When requesting personal information from employees, the College will generally comply with APP5 (Notification of the collection of personal information) by advising the employee that an employee's consent may be required if the College is seeking to collect their sensitive information, such as health or medical information.

Collection of personal information

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

Solicited Information

The College has, where possible, attempted to standardise the collection of personal information by using specifically designed forms. However, given the nature of the College's operations it also receives personal information by email, letters, notes, via the website, over the telephone, in face-to-face meetings, through financial transactions and through surveillance activities such as the use of CCTV security cameras or email monitoring.

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

The College may collect information based on how individuals use its 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 the website. This information is collected to analyse and improve the website, marketing campaigns and to record statistics on web traffic. The College does not use this information to personally identify individuals.

Unsolicited information

The College may be provided with personal information without having sought it through its 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 the College that are not in response to an advertised vacancy.
- Additional information provided to the College 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 the College will destroy, permanently delete or de-identify the personal information as appropriate.

Workplace Surveillance and Privacy

Different types of workplace surveillance such as monitoring email, internet and other computer resources will generally be exempt from the application of the Privacy Act.

The College has systems in place that:

- restrict access to certain types of websites.
- Monitor access to all websites including social media.
- Monitors email communication so that internal systems are not compromised.

CCTV Video Recording

Staff and students are aware that CCTV is used by the College for security purposes and by being at the College images may be recorded. CCTV is not installed in change rooms or toilets. Information from CCTV will only be used for security purposes and to assist with the inquiry into conduct concerns raised.

Collection and use of sensitive information

The College only collects sensitive information if it is:

- reasonably necessary for one or more of these functions or activities, and the College has the individual's consent.
- 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 organisation structure, but only if it is necessary for the College to provide its services.

How does the College use personal information?

The 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, or for an activity or purpose for which it has consent.

The College's primary use of personal information includes, but is not limited to:

- providing education, pastoral care, extra-curricular and health services.
- satisfying the College's legal obligations including its 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 Friends of Donvale.
- supporting the activities of the College.
- supporting community based causes and activities, charities and other causes in connection with the College's functions or activities.
- helping the College to improve its day-to-day operations including training its 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.

As part of the College's compliance with Part 6A of the Child Wellbeing and Safety Act 2005, the College may, or in some cases must, share information relating to the safety and wellbeing of children and young people with specific agencies or people. Despite laws prohibiting or restricting the disclosure of personal information, organisations and services prescribed as an "information sharing entity" (ISE), must share confidential information relating to the safety and wellbeing of a child or young person with other ISEs.

The College may share personal information to related bodies corporate, but only if necessary for the College 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 consent.

Storage and Security of Personal Information

The 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.

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.
- 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 the College's premises is secure at all times.
- Implementing physical security measures around the school buildings and grounds to prevent break-ins.
- Ensuring the College's 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 APPs or a similar privacy regime.
- The destruction, deletion or de-identification of personal information the College holds that is no longer needed, or required to be retained by any other laws.

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

Responding to data breaches

The College will take appropriate, 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 our 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, it will publish a statement on the 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 its functions or activities.

Personal information may be disclosed to government agencies, other parents, other schools, recipients of College publications, visiting teachers, counsellors and coaches, services 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:

- The College is 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 its 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 College has the individual's consent (which may be implied);
- The College is satisfied that the overseas recipient is compliant with the APPs, 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 is taking appropriate action in relation to suspected unlawful activity or serious misconduct.

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 takes a commonsense approach to dealing with a student's personal information and generally will refer any requests for personal information to a student's parents/carers. The College

will treat notices provided to parents/carers as notices provided to students and it will treat consents provided by parents/carers as consents provided by a student.

The College is however cognisant of the fact that children do have rights under the Privacy Act, and that in certain circumstances (especially when dealing with older students and especially when dealing with sensitive information), it will be appropriate to seek and obtain consents directly from students. The College also acknowledge that there may be occasions where a student may give or withhold consent with respect to the use of personal information independently from 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.

The quality of personal information

The 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 the Personal Information is incorrect or out of date, it will take reasonable steps to rectify the incorrect or out of date information.

Access and correction of personal information

An individual may submit a request to the College to access the personal information it holds, or request that it changes the personal information. Upon receiving such a request, the College will take steps to verify an individual's identity before granting access or correcting the information.

If the College rejects the request, an individual will be notified accordingly. Where appropriate, the College will provide the reason/s for its 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.

Complaints

An individual can make a complaint about how the College manages personal information, including a breach of the APPs or the Health Privacy Principles, 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 30 days), and it may seek further information in order to provide a full and complete response.

The College does not charge a fee for the handling of complaints. If an individual is not satisfied with the College's response, they can 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.

How to contact the College

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

- Emailing privacy@donvale.vic.edu.au
- Calling 03 9844 2471 and asking for the Privacy Officer
- Writing to our Privacy Officer at:
  155 Tindals Road, Donvale Vic 3111.

If practical, an individual can contact the College anonymously or by using a pseudonym. However, if an individual chooses not to identify themself, the College may not be able to give out the information or provide the assistance they might otherwise receive if it is not practical to do so.

Changes to the College's privacy and information handling practices

This Privacy Policy is subject to change at any time. Please check the Privacy Policy on the website www.donvale.vic.edu.au regularly for any changes.

Related Policies and Procedures

- Child Safety and Wellbeing Policy