



Privacy Policy

School Policy Contacts	
Responsible Officer	Principal
Policy Contact	Business Manager

Policy Governance	
Status	Approved
Version	1.0
Assigned Policy Group	Compliance
Approving Authority	EREA VSL Board EREA VSL CEO
Approval Date	9 February 2026
Effective Date	20 April 2026
Assigned Board Committee	Risk and Child Safety
Responsible Officer	EREA VSL CEO
Policy Owner	Risk and Compliance Manager
Review By	February 2028
Publication	School Policy Library School Website
Document Type	EREA VSL School Policy
Superseded Documents	Policy Program

1. Introduction

Edmund Rice Education Australia Victorian Schools Limited (EREA VSL) governs, conducts and manages registered non-government schools and school boarding premises in Victoria. It commenced as proprietor on 1 January 2024 and is focused on ensuring schools follow principles of good governance to maintain compliance with Australian and Victorian legislation and provide a safe environment for students and staff.

Parade College (the College) is committed to ensuring that personal information is collected, used, stored, and disclosed in a lawful and respectful manner. This includes taking reasonable steps to prevent unauthorised access, misuse, or disclosure of personal information that could constitute a serious breach of privacy.

The College observes the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth) including amendments introduced by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Privacy Amendment (Notifiable Data Breaches) Act 2017 and the Privacy and Other Legislation Amendment Act 2024 (Cth) (together referred to as “the Privacy Act”). In relation to health records, the College is bound by the *Health Records Act 2001* (Vic) and the Health Privacy Principles in that Act.

Where the College collects, uses or discloses personal information received from Victorian public sector bodies, or where the College is acting as an Information Sharing Entity under Victorian legislation, the College will also handle that information in accordance with the Information Privacy Principles set out in the *Privacy and Data Protection Act 2014* (Vic), to the extent applicable.

2. Purpose

The purpose of this document is to provide a framework for Parade College in dealing with privacy considerations. This policy provides a clear set of guidelines:

- for the collection, storage, use, disclosure, and disposal of personal information, including photos, videos, and health information at the College as a school of EREA VSL
- to ensure compliance with privacy legislation.

3. Scope

This policy applies to all personal and sensitive information (including health information) handled by Parade College

This policy is not applicable to information which is under the control of any third party to which the College provides personal information in accordance with this policy, except where the College has the right or power to deal with the information in the hands of the third party (for example, some technology service providers).

Under the *Privacy Act 1988* (Cth), 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 employee records unless required by law or organisational policy where the treatment is directly related to a current or former employment relationship between the College and the employee.

4. Principles

The following principles apply to the handling of personal information by Parade College

- personal information is managed in an open and transparent way

- only personal and / or sensitive information that is reasonably necessary for College functions or activities is collected
- fair and lawful means is used to collect personal information
- consent to collect sensitive information is obtained unless specified exemptions apply
- reasonable steps are taken to protect the personal information we hold from misuse, interference and loss and from unauthorised access, modification or disclosure
- personal information is only used or disclosed for the primary purpose of collection unless an exception applies.

5. Policy

5.1 Australian Privacy Principles and Victorian Privacy Obligations

The *Privacy Act 1988* (Cth) requires the College to handle any personal information (including 'sensitive' information) collected about individuals in accordance with the Australian Privacy Principles (APPs). The Policy must conform with the APPs found in the Act and with the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth).

In accordance with the APPs, our Privacy Policy outlines:

1. the **types of personal information collected** and held by the entity (APP1.4(a))
2. **how personal information is collected** and held (APP1.4(b))
3. the **purposes for which information is collected, held, used and disclosed** (APP1.4(c))
4. how an individual **may access their personal information and seek its correction** (APP1.4(d))
5. **how an individual may complain** if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP1.4(e))
6. whether the entity is likely to disclose **personal information to overseas recipients** (APP1.4(f)), and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy (APP1.4(g)).

5.2 Types of information collected

The College will only collect personal, sensitive (including health) information, if the information is reasonably necessary for one or more of its functions or activities. In the course of providing services and conducting its operations, and as part of recruitment processes, the College may collect and hold personal information, including sensitive information, about:

- staff members, job applicants, volunteers and contractors, including but not limited to:
 - name, contact details (including next of kin), date of birth, religion
 - information on job application
 - qualifications, registrations and professional learning history
 - salary and payment information, including banking and superannuation details
 - health information (e.g., details of disability and / or allergies, medical certificates)
 - national police check and working with children check
 - complaint records and investigation reports
 - leave details
 - photos and videos at school events

- workplace surveillance information, including CCTV footage
- work email and private email (when using work email address) and internet browsing history
- students, parents and carers ('parents') during and after the course of a student's enrolment at the College including but not limited to:
 - name, contact details (including next of kin), date of birth, gender, language background, previous school, religion
 - parents' education, occupation, language spoken at home, nationality and country of birth
 - health information (e.g., details of medical condition, disability and/or allergies, dietary requirements, absence notes, immunisation details, medical reports, names of doctors)
 - Victorian Student Number (VSN)
 - results of assessment tasks and other classroom activities
 - conduct and complaint records or other behaviour notes, and school reports
 - information about referrals to government welfare agencies
 - counselling reports
 - health fund details and Medicare number
 - any Family Court orders
 - criminal records
 - volunteering information
 - photos, videos at school activities, events and through closed circuit television (CCTV) if in use on school premises
- other people who come into contact with the College.

5.3 How personal information is collected

The College collects personal information in writing, through technology systems or in conversations, visits to the College, directly from the individual or from another source where reasonably required such as parents, contracted service providers or referrers.

Where the College collects health information, it will take reasonable steps to ensure that the individual is informed of the matters required by Health Privacy Principle 1 under the *Health Records Act 2001* (Vic), including the identity of EREA VSL, the purpose of collection, any legal authority for the collection, and the consequences (if any) of not providing the information.

In some circumstances, the College collects personal information from other sources, for example:

- from a school or entity related to the College
- a third party, such as a contracted service provider providing services to the College
- information provided to a third party by an individual for the purpose of sharing it with the College
- information sharing entities authorised by law
- CCTV systems which may be used in the College premises to provide safe environments for staff, students and visitors.

When visiting the College's digital platforms, the College may collect information about devices and activity. This includes the IP address, login information, browser type and version, time zone setting, operating system and platform, and the type of device. The College also 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 College website(s). This information is collected to analyse and improve the website, marketing campaigns and to record statistics on web traffic. This information is not used to personally identify individuals.

The 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 the College will, if able, destroy, permanently delete or de-identify the personal information as appropriate.

Individuals may interact with the College anonymously or under a pseudonym where it is lawful and practicable to do so. For example, if you contact the College with a general enquiry, you will not be required to provide your name unless it is necessary to appropriately respond to your request. However, in most interactions with the College, it will be necessary to collect your name, contact details,

and sufficient information relevant to the matter to ensure it is managed fairly and efficiently.

Anonymity is not possible during the student enrolment process or throughout a student's engagement with the College following successful enrolment.

5.4 How personal information is stored

The College stores personal information in a variety of formats including, but not limited to: databases; hard copy / paper files, personal devices (including laptop computers), and third party storage providers such as cloud storage facilities.

Personal information may also be stored by third parties outside our control, for example, information disclosed onto social media platforms that provide us with limited ability to store, modify or delete such information.

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 hard copy files are stored in lockable filing cabinets in lockable rooms. Staff access is subject to user role-based privilege
- ensuring access to premises is secured at all times
- implementing physical security measures around the College buildings and grounds to prevent break-ins
- ensuring our IT and cyber-security systems, policies and procedures are implemented and proactively monitored and subject to regular audits and testing
- 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 we hold that is no longer needed or required to be retained by any other laws
- in relation to health information, the College also takes reasonable steps to ensure that such information is accurate, complete, up to date and relevant to the purpose for which it is held or used.

The public websites of the College 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 cannot comment on their privacy policies.

5.5 Purposes for which information is collected, held, used and disclosed

Uses of personal information

The College only uses personal information for which it has received consent 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, or for the College activity or purpose.

The purpose of collecting and our primary uses of personal information include, but are not limited to:

- delivery of educational and pastoral services to the students enrolled in the College
- satisfying our legal obligations including our duty of care and child protection obligations
- marketing, promotional and fundraising activities
- supporting community-based causes and activities, charities and other causes in connection with our functions or activities
- helping us to improve our day-to-day operations including training staff
- systems development; developing new programs and services; undertaking planning, research and statistical analysis
- school administration including for insurance purposes
- employment of staff
- engagement of volunteers.

The College may disclose personal information, held about an individual to:

- state and federal government departments and authorities in relation to the regulation of schools
- medical practitioners and health service providers
- other schools with which the College interacts
- EREA VSL, the VCEA, Catholic education diocesan offices, and specialist visiting teachers
- third-party service providers that provide educational support and services to the College, including visiting teachers and specialist visitors, consultants, counsellors, sport coaches, providers of camps and excursions
- third parties providing services in relation to school improvement surveys or pastoral care services to the College and school system
- another school to facilitate the transfer of a student

- recipients of College publications, such as newsletters and magazines
- alumni and parent/friends support groups
- anyone who the College is required or authorised to disclose the information to by law, including under child protection and information-sharing laws.

The College prohibits any form of doxing which includes the intentional publication, sharing or threatening to disclose another's personal or identifying information without their consent.

If personal information is not collected, some services may be diminished or unable to be provided. We will only use or disclose sensitive or health information for a secondary purpose if it is reasonably expected of us to use or disclose the information and the secondary purpose is directly related to the primary purpose. Use of information may include the transmission of personal information from the College to EREA VSL and vice versa for the purposes of providing and promoting the activities and services of the College. We may share personal information with related bodies, but only if necessary for us to provide our services. We may disclose information about an individual to overseas recipients only when it is necessary, for example to facilitate a student exchange program.

Nationally Consistent Collection of Data (NCCD) on School Students with Disability

The Commonwealth Australian Education Regulation 2013 (the Regulations) require schools to provide the Commonwealth Department of Education (DoE) with certain information under the NCCD on students with a disability, including category of disability and level of adjustment. Schools collect the required information at an individual student level and may provide it to EREA VSL or other relevant organisations as Approved Authorities (for funding). Approved Authorities must comply with reporting, record keeping and data quality assurance obligations under the NCCD. Student information provided to the DoE for the purpose of the NCCD does not explicitly identify any student.

AI and Automated Decision-Making

Due diligence will be conducted to ensure any commercially available AI system employed by the College is suitable for its intended use. Every effort will be made to avoid using identifiable data however in circumstances where personal information is input into an AI system or automated decision-making tool, this will only be for the purpose for which the information was collected (in the case of sensitive information), or for a reasonably expected secondary use.

Circumstances where personal information may be used for automated decision-making include but are not limited to:

- analysis of student assessment and examination data
- recording and monitoring wellness data
- processing regular payment plans.

As a matter of best-practice, the College will not enter personal information into publicly available generative AI tools.

Sensitive information

The College may share sensitive information with other entities in our organisational structure, but only if it is necessary for us to provide our services.

Sensitive information includes a person's racial or ethnic origin, political opinion, religion, trade union or other professional or trade association membership, philosophical beliefs, sexual orientation or criminal record. The College will only collect information of this nature if it is reasonably necessary for its functions and activities and you consent, or it is lawfully authorised or obliged to collect such information.

Sensitive information will be used and disclosed by the College only for the purpose for which it was provided, or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the sensitive information is allowed by law.

The College will use the personal information it collects and holds for the primary purpose for which it was collected, which is to provide educational, co-curricular and related services to its students, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented.

Associated legislation and schemes

The College is an information sharing entity (ISE) in accordance with the Child Wellbeing and Safety (Information Sharing) Amendment Regulations 2020 (Vic). This legislation broadens the circumstances in which the College may share information to support the wellbeing and safety of children and students.

The College maintains appropriate confidentiality as it provides information under legislated information sharing schemes being the Child Information Sharing Scheme (CISS) and the Family Violence Information Sharing Scheme (FVISS), or under the *Terrorism (Community Protection) Act 2003* (Vic).

Where permitted or required by law, information may be shared under these schemes without the consent of the individual and, in some circumstances, without notifying the individual, where this is necessary to promote the safety or wellbeing of a child or to assess or manage family violence risk.

5.6 Disclosure of 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 APPs, 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 College will not send personal information about an individual outside Australia without your consent (in some cases this consent will be implied), and otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

The College is likely to only disclose personal information to overseas recipients if it is directly relevant to an overseas trip or excursion being undertaken by students and then only with the consent of the individual concerned (in which consent may be implied). It is not practicable to specify in this policy the countries in which the recipients of such information are likely to be located.

The Australian Government now has the authority to maintain a whitelist of overseas jurisdictions that are deemed to have privacy protections substantially similar to those under Australian law. Where personal information is disclosed to a recipient in a whitelisted jurisdiction, the College may rely on this status to satisfy its obligations under APP 8.1. Until such a whitelist is formally established and published, the College will continue to assess overseas disclosures on a case-by-case basis to ensure appropriate safeguards are in place.

5.7 Access to and correction of personal information

Under the *Privacy Act 1988* (Cth) and the *Health Records Act 2001* (Vic), an individual has the right to obtain access to any personal information which the College holds about them and may request correction of the information. However, there will be occasions when access is denied. Such occasions would include where release of the information:

- would have an unreasonable impact on the privacy of others
- may result in a breach of the school's duty of care to the student; or
- is unlawful.

Upon receiving such a request, the College will take steps to verify the requester's identity before granting access or correcting the information. The College may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested.

5.8 What happens when we no longer need your information?

The College will only keep your personal information for as long as needed for our purposes, or to comply with legislation that requires some information to be retained for certain periods of time. When we no longer require your information, we'll ensure that your information is destroyed or de-identified.

The College will retain certain records as part of an archival record of its schools, its former students, staff and the school communities for historic purposes.

5.9 Exception in relation to employee records

Under the *Privacy Act 1988* (Cth), 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 employee records unless required by law or organisational policy where the treatment is directly related to a current or former employment relationship between the College and the employee.

The College handles staff health records in accordance with the Health Privacy Principles in the *Health Records Act 2001* (Vic).

5.10 Enquiries and complaints

For further information about how the College manages the personal information it holds or if you wish to complain that you believe a breach of privacy has occurred, please contact the College on:

Email: Mark.Aiello@parade.vic.edu.au

Phone: 03 9468 3300

Website: [Complaints Handling Program](#)

The College can be contacted on an anonymous basis or by using a pseudonym. However, if you choose not to identify yourself, the College may not be able to provide the information or assistance you might otherwise receive if it is not practical to do so.

The College will investigate any complaint in accordance with our Complaints Management Policy and notify you of the outcome.

If you are not satisfied with our response, you 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 the OAIC should be a last resort once all other avenues of resolution have been exhausted.

Where a complaint relates to the handling of health information, an individual may also make a complaint to the Victorian Health Complaints Commissioner in accordance with the *Health Records Act 2001* (Vic).

6. Notifiable Data Breaches

6.1 Eligible Data Breach

Under APP 11 (security of personal information), the College is required to take reasonable technical and organisational measures to protect information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. These steps include but are not limited to staff training, password protocols and two factor authentication. The Notifiable Data Breach Scheme will require schools to notify the Office of the Australian Information Commissioner (OAIC) and the affected individual(s), in the event of a notifiable data breach.

The Office of the Australian Information Commissioner (OAIC) has regulatory powers under the *Privacy Act 1988* (Cth) to issue infringement notices, compliance notices, or directions where it identifies a failure to comply with privacy obligations. In cases of serious or repeated non-compliance, civil penalties may apply. The College takes its privacy responsibilities seriously and implements appropriate systems and safeguards to ensure ongoing compliance with the Australian Privacy Principles.

A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, or other misuse or interference. Pursuant to section 26WE of the Privacy Amendment (Notifiable Data Breaches) Act 2017, an eligible data breach, which would require notification, occurs in circumstances where:

- there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals (the affected individuals)
- a reasonable person would conclude there is a likelihood of serious harm to any affected individuals as a result
- the information is lost in circumstances where:
 - unauthorised access to, or unauthorised disclosure of, the information is likely to occur
 - assuming unauthorised access to, or unauthorised disclosure of, the information was to occur, a reasonable person would conclude that it would be likely to result in serious harm to the affected individuals.

Serious harm may include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

6.2 Response of the College

If the College suspects that an eligible data breach has occurred, it will carry out a reasonable and expedient assessment/investigation within 30 days using the Data Breach Response Plan. If such an assessment/investigation indicates there are reasonable grounds to believe an eligible data breach has occurred, then the College will report the breach to the EREA VSL Privacy Officer and will also be required to lodge a statement to the Privacy Commissioner (Commissioner). Where practical to do so, the College will also notify the affected individuals. If it is not practicable to notify the affected individuals, the College will publish a copy of the statement on its website or publicise it in another manner.

6.3 Exception to Notification Obligation

An exception to the requirement to notify will exist if there is a data breach and immediate remedial action is taken, and as a result of that action:

- there is no unauthorised access to, or unauthorised disclosure of, the information
- there is no serious harm to affected individuals, and as a result of the remedial action, a reasonable person would conclude the breach is not likely to result in serious harm.

7. Roles, Responsibilities and Reporting

Role	Responsibilities	Reporting
Principal	• Ensuring this policy and associated procedures are implemented in their school	EREA VSL CEO
College Privacy Officer	• Ensuring their school manages privacy and data in line with this policy and procedures • Providing appropriate support to staff at their school to understand and implement this Policy	Business Manager
School-level Data Breach Response Team	• Supporting the College Privacy Officer on the assessment of data breaches and immediate corrective actions • Recommending and implementing corrective actions for data breaches	Business Manager
EREA VSL Board	• Approving this policy • Reviewing compliance with this policy	

8. Review

This policy will be reviewed every two (2) years, or earlier if required due to changes in legislation, regulations, other requirements or after any significant incident.

9. Supporting Documents and Related Policies

This policy and procedures should be read in conjunction with the following related documents:

Supporting documents

- Data Breach Response Plan
- Collection Notice
- Employer Collection Notice
- [External Education Provider Policy and Procedures](#)

Related policies and documents

- EREA Code of Conduct

10. Legislation and Standards

- *Health Records Act 2001* (Vic)
- *Privacy Act 1988* (Cth)
- *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)

- *Privacy and Data Protection Act 2014 (Vic)*

11. Definitions

Term	Definition
Australian Privacy Principles (APPs)	The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the <i>Privacy Act 1988</i> (Cth) (Privacy Act). They apply to any organisation or agency the Privacy Act covers. There are 13 Australian Privacy Principles that govern standards, rights and obligations around: • the collection, use and disclosure of personal information • an organisation or agency’s governance and accountability • integrity and correction of personal information • the rights of individuals to access their personal information. The Australian Privacy Principles are principles-based law. This gives an organisation or agency flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies. A breach of an Australian Privacy Principle is an ‘interference with the privacy of an individual’ and can lead to regulatory action and penalties.
EREA VSL	Edmund Rice Education Australia Victorian Schools Limited. The proprietor of registered non-government schools and school boarding premises (EREA VSL Schools) in Victoria.
OAIC	Office of the Australian Information Commissioner
Personal Information	Personal information is information or an opinion that relates to 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, alumni, visitor, employee, member of the School Advisory Council and/or others who come into contact with the College.
Staff	The terms “staff” and “staff member” or “employee” include all teaching and non-teaching staff. They include all those employed by an EREA VSL School on a permanent, temporary or casual basis.