Privacy Policy

Introduction

Plenty River College (the College) is an independent specialist senior secondary College, delivering the Victorian Certificate of Applied Learning (VCAL) at Foundation, Intermediate and Senior levels. It provides a safe and inclusive learning environment for young people aged 15-20 years who may have been disengaged or are at risk of disengaging from education.

Plenty River College is a school of opportunities in which all students are empowered to achieve their personal best. Our mission is to assist students to develop life and work skills and achieve in their learning by:

- re-engaging them in education;
- fostering their social and emotional development; and
- providing a supportive and safe and environment for them.

Rationale

The College collects personal information about students, parents, staff and others to exercise its duty of care obligations, and to meet the educational and wellbeing needs of students. The College is committed to protecting the privacy of all information we collect, hold, manage, use, disclose and transfer. All employees, Board members and volunteers are required by law to protect the personal information the College collects and holds. All members of the College community have the right to understand how their personal information will be stored, used and disposed of.

Purpose

This purpose of this policy is:

- to assist College staff to understand the privacy requirements of Victorian and Commonwealth legislation;
- to make students and parents aware of how the College will collect, use, store and disclose their personal and other information; and
- to provide consistency in handling personal and other information within the College.

Scope

This policy applies to the Board, Executive Principal, Deputy Principal/Curriculum Leader, teaching staff, youth support workers, administration staff, parents and students at the College.

Definitions

Australian Privacy Principles (APPs)	The Australian Privacy Principles are a key component of the Privacy Act 1988 and are a set of set minimum standards which relate to the collection, security, storage, use, correction and disclosure of personal information and access to that information. It is mandatory for the College to comply with the Australian Privacy Principles (APPs).
Collection Notice	A statement provided to an individual at or before the time an organisation collects personal information from them (or if that is not practical, as soon as possible after the information is collected). A collection notice explains to individuals the purpose for which the information is collected, and how the organisation will use and handle the information.
Data breach	Unauthorised access to, or disclosure of, personal information, or a loss of personal information. Examples of a data breach include a lost or stolen device containing personal information, or mistakenly providing personal information to the wrong person.
Document	Anything on which there is writing, anything from which sounds, images, or writings can be reproduced, drawings or photographs
Health information	This is information or opinion about a person's physical, mental or psychological health, or disability, health status or medical history, whether recorded or not.
Notifiable data breach	A data breach that is likely to result in serious harm, which must be notified to affected individuals and the Australian Information Commissioner.
OAIC	Office of the Australian Information Commissioner
Personal information	Personal information is information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. It includes but is not limited to name, address, telephone number, email address, photographs, bank account details, assessment results, sex, marital status and parent/guardian details. In this policy personal information refers to personal information, health information and sensitive information unless otherwise specified.
Record	In the Privacy Act a 'record' includes a 'document' or an 'electronic or other device'. This definition excludes: a) a generally available publication (e.g. a telephone directory)

	b) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.
Sensitive information	Sensitive information is personal information about an individual's racial or ethnic origin, political opinions, membership or political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, sexual preferences, criminal record or health information. It includes, but is not limited to: health or disability information, racial or ethnic origin or working with children clearance information.
Victorian privacy law	Refers to the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic) collectively. There are additional Acts which have privacy implications for the College.

Responsibility

1. The College Board is responsible for authorising this policy.
2. The Executive Principal is responsible for:
    - implementing policies, procedures and processes to protect students and parent information privacy;
    - ensuring that personal information held at the College about a student or parent is up to date;
    - notifying the OAIC of a possible data breach;
    - the ongoing review of current information handling practices and security procedures to ensure compliance with this policy; and
    - training and informing staff of College information collection and handling practices.
3. Staff are responsible for:
    - ensuring the confidentiality and safety of personal information; and
    - ensuring personal information is kept up to date.
4. Students, Parents/Guardians are responsible for:
    - providing College with current and up to date information.

Implementation

Plenty River College is committed to privacy principles in state and federal legislation and ensure that the information of students, staff and parents is kept private and secure. The College has developed a Student Data Collection and Privacy Statement for use when collecting enrolment and other information (Please refer to ***Appendix 2***).

How Plenty River College collects personal information

The College collects, holds and uses a range of personal and health information, including sensitive information as is reasonably necessary for College operations. This includes:

- Students and parent information collected before, during and after enrolment;
- Information collected from staff members, volunteers, contractors and job applicants; and
- Information collected from Board Members.

The information is held in many forms such a student records, staff records, reports, paper files, electronic files.

The College uses a Collection Notice when requesting information directly from individuals.

Exception in relation to employee records:

Under the Privacy Act and the Health Records 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. The College handles staff health records in accordance with the Health Privacy Principles in the Health Records Act.

College use of personal information

1. Students and parents

The College primarily collects information to provide education services, exercise its duty of care, and perform necessary associated administrative activities.

2. Job applicants, volunteers and contractors

The College primarily collects information to assess and engage staff members or contractors, including checks on suitability and administering employment contracts.

3. Other uses

The College may use information to:

- obtain appropriate insurance;
- satisfy legal obligations (such as in relation to child protection legislation); and
- seek donations or market. the College

How the College treats sensitive information

Sensitive information will be used and disclosed 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.

Information disclosure

The College may disclose personal information held about an individual for education, administrative and support purposes to:

- other schools and teachers at those schools;

- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the College, including specialist visiting teachers, counsellors, social workers;
- providers of specialist advisory services and assistance to the College, including in the area of Human Resources, child protection and students with additional needs;
- assessment and educational authorities including Victorian Curriculum and Assessment Authority (VCAA), Victorian Regulations and Qualifications Authority (VRQA);
- agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes
- people providing administrative and financial services to the College
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

Sending information overseas

The College will not send personal information about an individual outside of Australia. In the unusual event that this occurs, the College will:

- obtain the consent of the individual; or
- otherwise comply with the Australian Privacy Principles or other applicable privacy legislation.

Management and security of personal information

The College takes reasonable steps to protect the personal information it holds from interference, misuse, loss, unauthorized access, modification and disclosure. These steps include but are not limited to:

- locked storage of paper records;
- security-protected access rights to electronic records;
- electronic backup of records;
- disposal of records in accordance with state and commonwealth legislation; and
- passwords access rights to emails

The College may use online or 'cloud' service providers to store personal information and to provide services to the College that involve the use of personal information, such as services relating to email, instant messaging and education and assessment applications. Some limited personal information may also be provided to these service providers to enable them to authenticate users that access their services. This personal information may be stored in the 'cloud' which means that it may reside on a cloud service provider's service which may be outside Australia.

Examples of such a 'cloud' service provider are Google (Google Classrooms, Gmail) and SIMON student management system.

Access and correction of personal information

Under the Commonwealth Privacy Act and the Health Records Act, an individual has the right to seek and obtain access to any personal information which the College holds about them, and to advise the College of any perceived inaccuracy. Students will generally be able to access and update their personal information through their parents if under 18 years.

To request to access or to update any personal information the College holds about you or your child, please contact the Executive Principal or the Administration staff by telephone or in writing.

The College may require you to verify your identity and specify what information you require. If we cannot provide you with access to that information, we will provide you with written notice explaining the reasons for refusal. This may include unreasonable impact on the privacy of others, or where the release may result in a breach of the College's duty of care to the student.

Consent and rights of access to the personal information of students

The College respects every Parent's right to make decisions concerning their child's education. Generally, the College will refer any requests for consent and notices in relation to the personal information of a student to the student's parent. The College will treat consent given by parents as consent given on behalf of the student, and notice to parents will act as a notice given to the student.

The College may, at its discretion and 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 parent. This would normally be done only when the maturity of the student and/or the student's personal circumstances warrant it.

Data Breaches

The College takes all data breaches seriously and will investigate the circumstances of loss, damage, unauthorised access or other breaches. The College will respond to data breaches according to its Data Breach Response Plan (please refer to ***Appendix 1***). Data breaches likely to result in "serious harm" to an individual such as physical, psychological, emotional, financial or reputational harm will be reported to the Office of the Australian Information Commissioner in accordance with the National Data Breaches Scheme requirements.

Enquiries and complaints

If you would like further information about the way the College manages personal information it holds, or wish to complain that you believe that the College has breached the Australian Privacy Principles please contact the Executive Principal by writing to **admin@prc.vic.edu.au.** The College will investigate any complaint and will notify you of the making of a decision in relation to your complaint as soon as is practicable after it has been made.

Communication

1. This policy will be communicated to the College community through the College website.

2. College teaching and education support staff will be informed of their obligations in relation to this policy by:
    - attending the College induction program for new staff;
    - receiving a copy of this policy at the first staff meeting at start of the College year;
    - receiving a copy of the College's Teacher Handbook.

Appendices:
Appendix 1: Plenty River College Data Breach Response Plan Appendix 2: Student Data Protection and Privacy Statement
Related Policies:
• Accident and Incident Reporting • Accuracy and Integrity of Student Records • Administration of Medication • Anaphylaxis • Assessment and Reporting • Attendance • Bullying and Harassment Prevention • Camps and Excursions • Child Safe • Enrolment • External Providers • First Aid • Health Care Needs • Mandatory Reporting • Student Behaviour Management • Student Engagement, Wellbeing and Inclusion
Related Legislation
• Education and Training Reform Act 2006 (Vic) • Education and Training Reform Regulations 2017 (Vic) • Health Records Act 2001(Vic) • Privacy Act 1988 (Cth) • Privacy and Data Protection Act 2014 (Vic)

Appendix 1: Plenty River College Data Breach Response Plan

	Procedure: Data Breach Response Plan

Purpose

To set out procedures to implement the mandatory notifiable data breaches scheme that applies under the Privacy Act 1988.

Procedure

1. Identification of a breach

   i. The College experiences data breach or a data breach is suspected: This may be discovered by a staff member, or a staff member may be alerted by another party or system.

   ii. When a staff member discovers a known or suspected data breach they should immediately notify the Executive Principal. Please provide as much information as possible such as the time and date the known or suspected breach was discovered, the type of personal information involved, the cause and extent of the breach, and the context of the affected information and the breach.

   iii. Any immediate steps available to contain the breach must be identified and implemented in discussion with the Executive Principal. Reducing the scale and impact of a data breach can prevent the need for notification to the OAIC. All known or suspected data breaches must still be notified internally to the Executive Principal.

2. Assessment of a breach

   i. Not all data breaches are notifiable. If, after an initial investigation, the Executive Principal suspects a notifiable data breach may have occurred, a reasonable and expeditious assessment must be undertaken to determine if the data breach is likely to result in serious harm to any individual affected

   ii. The Executive Principal will seek information to assess the suspected breach. In assessing a suspected breach, the Executive Principal may require assistance and information from other areas of the College depending on the circumstances.

   iii. There will then be an evaluation of the scope and possible impact of the breach. The Executive Principal will assess if a breach is likely to be notifiable and ensure appropriate actions including reporting to the Office of the Australian Information Commissioner (OAIC). An assessment of a known or suspected breach must be conducted expeditiously and where possible should be completed within 30 days.

iv. In all cases the assessment will identify what actions must be taken. These will be documented and acted upon as soon as possible.

v. There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

vi. There are four key steps to consider when responding to a breach or suspected breach.
STEP 1: Contain the breach and do a preliminary assessment
STEP 2: Evaluate the risks associated with the breach
STEP 3: Notification to OAIC and affected individuals
STEP 4: Prevent future breaches

3. A notifiable breach

i. A breach which is assessed as likely to result in serious harm to individuals whose personal information is involved, is a notifiable data breach. Such data breaches must be notified to the affected individuals and the OAIC. Notice must include information about the breach and the steps taken in response to the breach.

ii. If the College has responded quickly to the breach, and as a result of this action the data breach is not likely to result in serious harm, there is no need to notify individuals or the OAIC. However, the College may decide to tell the affected individuals about the incident if it is considered appropriate

iii. The risk of serious harm will be assessed by considering both the likelihood of the harm occurring and the consequences of the harm. Some of the factors that should be considered are:

Factors	**Considerations**
The type of personal information involved in the data breach	Some kinds of personal information are more sensitive than others and could lead to serious ramifications for individuals if accessed. Information about a person's health, documents commonly used for identity fraud (e.g. Medicare card, driver's licence) or financial information are examples of information that could be misused if the information falls into the wrong hands.
Circumstances of the data breach	The scale and size of the breach may be relevant in determining the likelihood of serious harm. The disclosure of information relating to a large number of individuals would normally lead to an overall increased risk of at least some of those people experiencing harm. The length of time that the information has been accessible is also relevant. Consideration must be given to who may have gained unauthorised access to information, and what their intention

	was (if any) in obtaining such access. It may be that there was a specific intention to use the information in a negative or malicious way.
Nature of possible harm	Consider the broad range of potential harm that could follow from a data breach including: • identity theft • financial loss • threat to a person's safety • loss of business or employment opportunities and • damage to reputation (personal and professional).

iv. Notification to the OAIC and internally within the College is the responsibility of the Executive Principal

v. Notifications will follow the format identified by the OAIC in *Data breach preparation and response.*

4. Response Team
   A response team will be formed for a serious breach. The team will include the Executive Principal, IT staff, the Business Manager. The team may seek advice from the Board's legal representative.

5. Breaches that are not serious

   Breaches that are not assessed as serious may be handled by management team but must be reported to the Executive Principal

6. Records
   Documentation will be stored for each suspected breach.

Appendix 2: Student Data Protection and Privacy Statement

Student Data Protection and Privacy Collection Statement

Plenty River College is committed to protecting the privacy of all information we collect, hold, manage, use, disclose and transfer.

As a student of the College, we will keep a record of the details you provided in your application and any supporting documents requested as part of your admission, and additional information collected in the course of your studies with us. This will become part of your student record. Your student record also includes information about your academic progress and outcomes.

The personal data processed by us as part of your student record will include details such as your name, home address, date of birth, course studied, fee payments, financial aid, health and wellbeing support. It will also include unique personal identifiers assigned to you (e.g. your student number) and details of any disciplinary or conduct issues. Access to, and the sharing of, this type of data are controlled very carefully.

Where you provide the College with the personal data of others (e.g. emergency contact details) you are encouraged to inform them that:

- you are disclosing that information to the College;
- the information will be retained; and
- they can access that information by contacting the Executive Principal.

Your personal data is created, stored and transmitted securely in a variety of paper and electronic formats. Access to your personal data is limited to the College staff or affiliates who have a legitimate interest in it for the purpose of carrying out their duties.

The personal data processed by us, or processed on our behalf, is needed for the purpose of your enrolment and throughout the time you are with us as a student and to help the College improve your experience as a student. If you choose not to provide your personal data, it may not be possible for the the College to enrol you, or provide you with support to complete your course of study, and may limit opportunities available to you.

The specific purpose for processing personal data outside of your student record will be communicated to you at the time that we first interact with you. If you choose not to provide your personal data, it may not be possible for the College to provide you with the specific information, assistance, facilities or services that you have requested.

We consider that the lawful basis for the processing of your personal data as a student of the College is that it is necessary for the pursuit of the legitimate interests of the College to provide you with the course of study to which you are enrolled.

We will obtain your consent for specific use of your personal data not covered by this Student Data Protection and Privacy Collection Statement or where that personal data includes special category data (e.g. as identified above), which we will collect from you at the appropriate time. You can withdraw your consent to our specific use of such data at any time.

In addition to the purposes set out in the Privacy Policy, our specific processing purposes of your personal data as a student and how we use it include:

- to correspond with you;
- to attend to day to day administrative matters;
- to inform you about your courses and other events related to your course;
- to facilitate and enable programs relevant to your studies such structured workplace learning or work experience;
- to enable participation at events e.g. Presentation Night;
- to facilitate and enable opportunities in community engagement, work-integrated learning activities and student-to-student learning;
- to seek feedback of your experience as a student with us;
- for benchmarking, analyses, quality assurance and planning purposes;
- to compile statistics and conduct research for internal and statutory reporting purposes;
- to fulfil and monitor our responsibilities to comply with legislative reporting requirements; and
- to use the information as otherwise permitted by the law other schools and teachers at those schools.

Our student wellbeing support services

We make wellbeing support services available to our students. If you receive wellbeing support from us, we may collect additional personal information about you, including health information about you, as part of providing this service. Health information includes any information or an opinion about an individual's physical, mental or psychological health, any disability that an individual has and any details of any health or medical services provided to an individual.

We will only collect health information about you with your consent. Our use and management of that information will be explained in the relevant privacy collection notices specific to those services.

Health and personal information about you collected for these services will only be used for the purpose of providing the services to you. Any wellbeing support service that we provide is confidential and any information that you provide to us will be held in the strictest confidence. Any health information that we collect about you will be separately stored by our support staff and will not form part of your student records.

Sharing of your information

The College may disclose your personal information to:

- other schools and teachers at those schools;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the College, including specialist visiting teachers, counsellors, social workers;
- providers of specialist advisory services and assistance to the College, including in the area of Human Resources, child protection and students with additional needs;
- assessment and educational authorities including Victorian Curriculum and Assessment Authority (VCAA), and the Victorian Regulations and Qualifications Authority (VRQA);
- agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes;
- people providing administrative and financial services to the College; and
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

Where personal data is disclosed to third parties, it will be done so only to the extent necessary to fulfil the purpose of such disclosure.

How we keep your information secure

Your personal information is created, stored and transmitted in a variety of paper and electronic formats.

We take reasonable steps to ensure that any personal information we collect, transmit, store or otherwise process, is accurate and complete, and that appropriate measures are implemented and maintained to protect it from accidental or unlawful destruction, misuse, loss, alteration, or unauthorised access or disclosure.

Your academic record is retained indefinitely so that the details of your academic achievements can be confirmed and for statistical or historical research purposes.

Your individual rights

In addition to your rights to access and correct your personal data and lodge a complaint relating to how we handle your personal data as set out in the Privacy Policy, you may, under certain conditions, have the following rights available:

- to object to any processing of your personal data that we process on the lawful basis of legitimate interests, unless our reasons for the underlying processing outweighs your interests, rights and freedoms;
- to withdraw your consent where we have processed any of your personal data based on consent;
- to object to direct marketing (including any profiling) at any time;
- to ask us to delete personal data that we no longer have lawful grounds to process; and

- to object to the use of automated decision making.

If you have any questions about how your personal data is being used, or you wish to exercise any of your individual rights that are available to you, please contact the Executive Principal by writing to admin@plentyrivercollege.gmail.com.