

Privacy Policy

Scope

This policy applies to Bairnsdale Christian College (BCC).

Statement

Bairnsdale Christian College collects and stores data in association with its operation as a school and as a business. The purpose of this policy is to outline the type of information that the School collects, the manner in which the data is collected, and the procedures that the School has in place to protect its data.

The School complies with the requirements of the Privacy Act 1988 & the 13 Australian Privacy Principles.

Procedures

Data Collection

The School collects:

1. Personal Information including names, addresses and other contact details; dates of birth; next of kin details; financial information, photographic images and attendance records.
2. Sensitive Information (particularly in relation to student and parent records) including religious beliefs, government identifiers, nationality, country of birth, languages spoken at home, professional memberships, family court orders and criminal records.
3. Health Information (particularly in relation to student and parent records) including medical records, disabilities, immunisation details, individual health care plans, counselling reports, nutrition and dietary requirements.
4. Personal information you provide - The School will generally collect personal information held about an individual by way of forms filled out by parents or students, face-to-face meetings, interviews, telephone calls etc.
5. Personal information provided by others - In some circumstances the School may be provided with personal information about an individual from a third party, e.g. a report provided by a medical professional or a reference from another School.
6. Digital Information from devices connected to the BCC network such as Facebook, Instagram & Twitter messages and the content of emails and internet traffic. All data sent and received across the BCC network is monitored for

trigger words and phrases related to possible self-harm, offensive, or discriminatory themes, topics and statements.

7. Information on the use of facilities from surveillance cameras, access controls, and other on premises systems.

Closed Circuit Television (CCTV)

The College uses CCTV systems to support the safety and security of students, staff, visitors, and property. CCTV images may constitute personal information and will be managed in accordance with this Privacy Policy.

Purpose of CCTV

- Promote the health, safety, and welfare of students, staff, and visitors.
- Safeguard College buildings and equipment.
- Prevent, detect, and investigate incidents, including crime, anti-social behaviour, or other inappropriate conduct.
- Provide situational awareness and visual coverage in emergencies.

Live CCTV Footage

Live CCTV footage may be accessed by authorised staff to:

- Provide situational awareness of incidents posing a risk to health or safety, or following an alarm activation or other trigger.
- Monitor activities where there is a reasonable belief that an incident will occur and monitoring will help to identify the persons involved and/or reduce risk.
- Support emergency management.

Recorded CCTV Footage

Recorded CCTV footage may be accessed by authorised staff to:

- Prevent, verify, and investigate incidents involving criminal behaviour, staff misconduct, or inappropriate behaviour.
- Verify and investigate incidents involving injury, loss, or damage.
- Support College leadership with incident review and debriefing.

Prohibited Locations of CCTV Cameras

CCTV cameras will not be installed in areas where individual privacy is paramount, including:

- Toilets
- Change rooms
- Dressing rooms
- Showers
- Any other location where there is a reasonable expectation of privacy.

Additional Requirements

- The Principal must approve all access to live or recorded footage.
- The State Executive Officer must be consulted prior to using CCTV footage for staff misconduct or discipline-related matters.
- CCTV does not record audio.
- CCTV will not be used for routine staff performance monitoring.
- Signage will be displayed at campus entry points to inform the community that CCTV is in use.

See Data Storage and Security for additional procedures.

Data Usage

The School uses data:

1. To keep parents informed about matters related to their child's schooling, through correspondence, newsletters, magazines and reports
2. For the day-to-day School administration
3. To support the student's educational, social and medical well-being
4. To improve School systems and procedures
5. To develop marketing and implement marketing strategies
6. To satisfy the School's legal obligations and allow the School to discharge its duty of care
7. To assist in matters relating to staff and student conduct.

Data Storage & Security

The School stores personal information in a variety of formats including on cloud databases, on hard copy files, and on devices including laptop computers, mobile phones, cameras and other recording devices.

The security of your personal information is of importance to us and we take all reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure.

The College uses Artificial Intelligence across its Core Technology Platforms. Direct access to LLMs is through licensing agreements that prohibit the use of company data for the purpose of training the LLM.

CCTV footage is stored securely for a limited period (approximately four weeks) unless required longer for investigation.

A register of all access to CCTV recordings will be maintained.

Disclosure of Information

The School may disclose personal information, including sensitive information, held about an individual to:

1. Another colleague as required
2. Government departments
3. Medical practitioners
4. People and/or companies providing services to the School
5. Recipients of School publications (newsletters, magazines)
6. Parents and anyone you authorise the School to disclose information to.
7. Related organisations
8. 3rd-party providers of services to the school

Sensitive Information

Sensitive information means: Information relating to a person's racial or ethnic origin, political opinions, religion, trade union or other professional or trade association membership, sexual preferences or criminal record and health information.

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

Disclosure of personal information to overseas recipients

The School may disclose personal information about an individual to overseas recipients in certain circumstances, such as when we are organising an overseas excursion, facilitating a student exchange, or storing information with a "cloud computing service" which stores data outside of Australia.

Review of Data

The School endeavours to ensure that the personal information it holds is accurate, complete and up-to-date. A person may seek to update their personal information held by the School by contacting the School administration at any time.

Notification of Data Breach

If the School suspects that a data breach has occurred, it will carry out a reasonable and expedient assessment/investigation within 30 days. If such an assessment/investigation indicates there are reasonable grounds to believe an eligible data breach has occurred, then the School will lodge a statement to the Privacy

Commissioner. Where practical to do so, the School will also notify the affected individuals. If it is not practicable to notify the affected individuals, the School will publish a copy of the statement on its website, or publicise it in another manner unless there is no unauthorised access to, or unauthorised disclosure of the information or 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.

Access to Personal Data

Under the Commonwealth Privacy Act, an individual has the right to obtain access to any personal information which the School holds about them and to advise the School of any perceived inaccuracy.

Requests to access any information the School holds about individuals are to be made in writing to the Principal. The School may require you to verify your identity and specify what information you require.

The School will charge an hourly fee to cover the cost of verifying your application and locating, retrieving, viewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

A parent may seek access to personal information held by the School about them or their child by contacting the Principal. However, there will be occasions when access is denied pursuant to exceptions under the Privacy Act.

Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or a court order, or where the release may result in a breach of the School's duty of care to the student.

Referral Process

An individual whose personal information is/has been held by the School may lodge a complaint in writing to the Principal about an act or practice of the School which the individual believes to be inappropriate or unlawful.

The principal will investigate the complaint and a decision will be made concerning the complaint and the complainant will be advised in writing of the result of the investigation within 30 days of the complaint.

Should the complainant be dissatisfied with the School's response, the complainant can make a complaint to the Office of the Australian Information Commissioner.

Policy Implementation Information	
Legislation	<p>The Australian Privacy Principles from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012</p> <p>Privacy Act 1988 (Cth)</p>
Board Approval	August, 2025
Review	3 years