



*With Jesus Christ as our inspiration and guide, we are called to provide high-quality Catholic education in the Diocese of Bathurst'*

## PRIVACY POLICY

---

### 1. MISSION AND VALUES

In partnership with the family, parish and community, our schools nurture a relationship with God in Christ Jesus, celebrate and share the Catholic faith, and educate to enable all to make a positive contribution to the world.

We are therefore committed to:

- a safe, inclusive and professional learning environment
- just and right relationships that recognise and respect the dignity of each individual
- a commitment to continuous improvement, innovation and evaluation of performance.

### 2. PURPOSE

The purpose of this document is to clarify the agreed practices at Catholic Education Diocese of Bathurst (CEDB) in relation to Privacy for all staff, students, parents, guardians, as well as volunteers, religious and contractors. This Policy ensures that

- CEDB and schools comply with the Privacy Act
- Personal, health and sensitive information is held and handled in accordance with the Privacy Act
- Guidance is provided on the responsible handling and storage of all personal information
- Information on how to access information is available

### 3. EXPECTATIONS

It is expected that all staff at CEDB will adhere to the scope and procedures outlined in this document as these are the agreed practices of the CEDB and schools. If an issue arises in relation to these practices, please see the individual responsible for overseeing this area so the issue can be addressed in an appropriate and timely manner. A local policy is not required.

It is expected that all personnel will

- Abide by the National Privacy Principles contained in the Commonwealth Privacy Act
- Be informed of this policy annually by the School Principal or Team Leader at CEDB

### 4. DEFINITIONS

**Personal information** means information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source.

**Sensitive information** is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record. It also includes health information and biometric information.

**Health information** is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service

**Records** The Privacy Act regulates personal information contained in a 'record'. A 'record' includes a 'document' or an 'electronic or other device'. The definition is inclusive and therefore covers a wide variety of material which might constitute a record and includes documents, databases, pictures or pictorial representations.

**Solicited Information** is collected through specific forms (e.g. enrolment applications, Job Applications), as well as by email, letters, notes, via websites, 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.

Personal information can be collected from other people or independent sources. However, only where it is not reasonable and practical to collect the personal information from the individual directly.

**Unsolicited information** may be provided without having sought it through normal means of collection and is often collected by:

- Misdirected postal mail – Letters, Notes, Documents;
- Misdirected electronic mail – Emails, electronic messages;
- Employment applications that are not in response to an advertised vacancy;
- Additional information provided which was not requested.

## 5. GUIDELINES

This Privacy Policy applies to Catholic Education Diocese of Bathurst and schools conducted by CEDB and sets out how CEDB and each school manages personal information provided to or collected by it. CEDB and schools are bound by the Australian Privacy Principles contained in the Commonwealth Privacy Act. In relation to health records CEDB and schools are also bound by the Health Records and Information Privacy Act 2002 (Health Records Act).

### **What kinds of personal information is collected and how is it collected?**

The type of information collected and held includes (but is not limited to) personal information, including health and other sensitive information, about:

- pupils and parents and/or guardians (Parents) before, during and after the course of a pupil's enrolment at the school;
- job applicants, staff members, volunteers and contractors; and
- other people who come into contact with the CEDB or school.

Personal parent and student information collected and held will vary depending on the context of the collection and may include but is not limited to:

1. Personal Information including names, addresses and other contact details; dates of birth; next of kin details; photographic images; educational information, attendance records and financial information.
2. Sensitive Information (particularly in relation to student and parent records) including government identifiers (such as TFN), religious beliefs, nationality, country of birth, 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 and psychological reports.

As part of recruitment processes for employees, contractors and volunteers, information collected and held may include but is not limited to:

4. 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.
5. Sensitive Information including government identifiers (such as TFN), nationality, country of birth, professional memberships, family court orders and criminal records.
6. Health Information (particularly in relation to prospective staff) including medical records, disabilities, and immunisation details.

Generally, where personal information is directly collected from an individual, consent is obtained from the individual in writing before collection (including health information).

Note that records relating to employees employed by CEDB are not covered by the APPs or the Health Privacy Principles where they relate to current or former employment relations between CEDB and the employee.

Personal Information provided by a staff member, parent or student: Generally collection of personal information, held about an individual, is by way of forms, face-to-face meetings and interviews, emails and telephone calls.

Personal Information provided by other people: In some circumstances information may be provided about an individual from a third party, for example a report provided by a medical professional or a reference from another school.

Exception in relation to employee records: Under the *Privacy Act 2002* and *Health Records and Information Privacy Act 2002 (NSW)*, the Australian Privacy Principles and Health Privacy Principles do not apply to an employee record. As a result, this Privacy Policy does not apply to the School's treatment of an employee record, where the treatment is directly related to a current or former employment relationship between the school and employee.

#### **How will the personal information provided be used?**

Personal information is collected for the primary purpose of collection, and for other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which an individual has consented.

Pupils and Parents: In relation to personal information of pupils and parents, the primary purpose of collection is to enable the school to provide schooling for the pupils enrolled at the school, exercise its duty of care, and perform necessary associated administrative activities, which will enable pupils to take part in all the activities of the school. This includes satisfying the needs of parents, the needs of the pupil and the needs of CEDB and school throughout the whole period the pupil is enrolled at the school.

The purposes for which CEDB and a school uses personal information of pupils and parents include:

- to keep parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- day-to-day administration;
- looking after pupils' educational, social, spiritual and medical wellbeing;
- seeking donations and marketing for the school;
- to satisfy CEDB and the school's legal obligations and allow the school to discharge its duty of care;
- complying with Governmental obligations at both Federal and State level ;
- responding to the needs of parents, students and school communities;
- marketing, promotional and fundraising activities;

- systems development; developing new programs and services; undertaking planning, research and statistical analysis;
- the employment of staff; and
- the engagement of volunteers.

In some instances where a school requests personal information about a pupil or parent, if the information requested is not obtained, the school may not be able to enrol or continue the enrolment of the pupil or permit the pupil to take part in a particular activity.

**Job applicants, staff members and contractors:** In relation to personal information of job applicants, staff members and contractors, the CEDB or school's primary purpose of collection is to assess and (if successful) to engage the applicant, or contractor, as the case may be.

The purposes for which a school or CEDB uses personal information of job applicants and contractors include:

- for insurance purposes;
- seeking funds and marketing;
- to satisfy CEDB and the school legal obligations, for example, in relation to child protection legislation;
- complying with Governmental obligations at both Federal and State level;
- facilitating opportunities to collaborate on education related matters;
- improving day-to-day operations including training of staff;
- systems development including developing new programs and services, undertaking planning, research and statistical analysis;
- the employment of staff; and
- the engagement of volunteers.

**Volunteers:** CEDB and schools obtain personal information about volunteers who assist the CEDB and school in its functions or conduct associated activities, such as Parents and Friends Associations, to enable the school and the volunteers to work together.

**Marketing and fundraising:** Marketing and seeking donations for the future growth and development of the school is an important part of ensuring that the school continues to be a quality learning environment in which both pupils and staff thrive. Personal information held by a school may be disclosed to an organisation that assists in the school's fundraising, for example, the school's Parents and Friends Association.

Parents, staff, contractors and other members of the wider school community may from time to time receive fundraising information. School publications, like newsletters and magazines, which include personal information, may be used for marketing purposes.

**Exception in relation to related schools:** The Privacy Act allows each school, being legally related to each of the other schools conducted by CEDB, to share personal (but not sensitive) information with other schools conducted by CEDB. Other CEDB schools may then only use this personal information for the purpose for which it was originally collected by CEDB. This allows schools to transfer information between them, for example, when a pupil transfers from a CEDB school to another school conducted by CEDB.

### **Who might personal information be disclosed to?**

The CEDB or School may disclose personal information, including sensitive information, held about an individual for educational, administrative and support purposes. This may include 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 School, including specialist visiting teachers, [sports] coaches, volunteers, and counsellors;

- providers of specialist advisory services and assistance to the School, including in the area of Human Resources, child protection and students with additional needs;
- providers of learning and assessment tools;
- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- people providing administrative and financial services to the School;
- recipients of School publications, such as newsletters and magazines;
- pupils' parents or guardians;
- anyone authorised by the School to disclose information to; and
- anyone to whom CEDB or school are required or authorised to disclose the information to, by law, including child protection laws.

CEDB and schools may disclose personal information without consent or in a manner which an individual would reasonably expect if:

- 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.

### **Sending information overseas**

The CEDB or School may disclose personal information about an individual to overseas recipients, for instance, to facilitate a school exchange. However, the School will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the Australian Privacy Principles or other applicable privacy legislation.

### **Storage and security of personal information**

CEDB and schools store 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; and
- paper based files.

CEDB and schools take all reasonable steps to protect the personal information held from misuse, loss, unauthorised access, modification or disclosure.

These steps include, but are not limited to:

- Restricting access and user privilege to information by employees
- Ensuring employees do not share personal passwords.
- Ensuring hard copy files are stored in lockable facilities
- Employee access is subject to user privilege.
- Ensuring access to CEDB and school premises are secured.
- Implementing physical security measures around the premises.
- Ensuring IT and cyber security systems, policies and procedures are implemented and up to date.
- Ensuring employees comply with 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 held that is no longer needed or required to be retained by any other laws.

### **Storing information overseas**

The CEDB or School may use online or 'cloud' service providers to store personal information and to provide services to the School 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 servers which may be situated outside Australia.

### **Responding to data breaches**

Data breaches or suspected data breaches are dealt with by the Data Trustees for CEDB and the *Data Breach Guidelines*.

### **How does the school treat personal 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.

## **6. PROCEDURES**

### **Management and security of personal information**

CEDB's and the schools' staff are required to respect the confidentiality of pupils' and Parents' personal information and the privacy of individuals.

Each school has in place steps to protect the personal information the school holds from misuse, interference and loss, unauthorised access, modification or disclosure by use of various methods including restricted access, locked storage of paper records and password access rights to computerised records.

### **Access and correction of personal information**

Under the *Commonwealth Privacy Act* and *Health Records Act*, an individual has the right to seek and obtain access to personal information which CEDB or a school holds about them and to advise CEDB or the school of any perceived inaccuracy. There are some exceptions to this right set out in the Act. Pupils will generally be able to access and update their personal information through their parents, but older pupils may seek access and correction themselves.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access or update any personal information CEDB or a school holds, written contact is to be made with the CEDB or school's Principal.

The CEDB or school may require verification of identity and clarification of the information required.

The CEDB or school may charge a fee to cover the cost of verifying, locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the CEDB or school will advise the likely cost in advance. If access to the specific information is not available, a written notice explaining the reasons for refusal will be provided. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the school's duty of care to the pupil.

A school may, at its discretion, on the request of a pupil, grant that pupil access to information held by the school about them, or allow a pupil 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 pupil and/or the pupil's personal circumstances warranted it.

### **Consent and rights of access to the personal information of pupils**

CEDB respects every parent's right to make decisions concerning their child's education.

Generally, a school will refer any requests for consent and notices in relation to the personal information of a pupil to the pupil's parents. A school will treat consent given by parents as consent given on behalf of the pupil, and notice to parents will act as notice given to the pupil.

### **Enquiries and complaints**

Schools are also required to advise individuals in their Privacy Policy of how they may complain about a breach and how the School will deal with that complaint. Schools should ensure that their Privacy Policy correctly reflects their procedures for dealing with complaints. Schools are required to advise individuals in their collection statement that their Privacy Policy contains this information.

Information about the way CEDB or a school manages the personal information it holds, is obtainable from CEDB or the school. Complaints regarding breaches of the Australian Privacy Principles, should be made by initially contacting the school's Principal or then CEDB. The school and/or CEDB will investigate any complaint and will notify the complainant of a decision in relation to the complaint as soon as is practicable after it has been made.

### **Privacy Officer**

Schools, especially larger schools, may consider nominating an individual as the Privacy Officer for the school. A privacy officer can be the first point of contact for internal and external queries on privacy matters and coordinates a School's privacy compliance. They may also conduct privacy training. Everyone at the School should be made aware who the privacy officer is.

### **Photographs and videos of students**

Information and guidance on photography and videos of students can be obtained in Chapter 26 and Annexure 5 of the CSNSW Schools Privacy Compliance Manual. This clarifies when consent is NOT required, how and when general and specific consent should be gathered, and other matters.

### **Data Breach**

Data Breach responses should be aligned with the Diocesan Data Breach Response Guidelines.

### **How should information be exchanged under Chapter 16A be handled and stored?**

Information must be handled and stored in a secure way. A written record of exchanges of information under Chapter 16A should be made and stored in a way that is consistent with the existing legislation (including the *State Records Act 1998*, *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Protection Act 2002*).

## **7. LEGISLATIVE FRAMEWORK**

*Privacy Act 1988* (Commonwealth)  
*State Records Act 1998*  
*Privacy and Personal Information Protection Act 1998*  
*Health Records and Information Privacy Act 2002* (NSW)  
*Privacy Amendment (Enhancing Privacy Protection) Act 2012*  
*Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)

## **8. RELATED POLICIES AND GUIDELINES**

*Data Breach Guidelines* Catholic Education Diocese of Bathurst  
*Child Protection Policy* Catholic Education Diocese of Bathurst  
*Enrolment Policy* Catholic Education Diocese of Bathurst  
*Guidelines in the Professional Conduct in the Protection of Children and Young People*  
*Complaints Guidelines* Catholic Education Diocese of Bathurst  
*Enrolment of Students with Additional Learning Needs* Catholic Education Diocese of Bathurst  
*Recruitment of Staff Policy* Catholic Education Diocese of Bathurst  
*Schools Privacy Compliance Manual* Catholic Schools NSW



## 9. POLICY ADMINISTRATION

This policy has been ratified by the Executive Director of Schools and will be reviewed periodically, or in the event of any information or incident that indicates the need for a review, or following relevant legislative , new technology, changes to operational practices and procedures or organisational change.

It is the responsibility of anyone accessing this document to ensure that the current version is downloaded from CEDB website.

Date of Implementation	2009
Date of Last Review	2019
Date for Next Review	2022

### Appendix

- Appendix 1     Summary of Schools Obligations
- Appendix 2     Counselling Disclosure Statement