

## Privacy Policy

### Related Policies and Documents and Acts

---

Privacy Act 1988 (Cth)  
Information Privacy ACT 2014 (ACT)  
Records and Information Privacy Act 2002 (NSW)  
Health Records (Privacy and Access) Act (ACT)  
Confidentiality Policy

### Purpose

---

This Privacy Policy details how we protect your privacy and how we comply with the requirements of the Privacy Act and the 13 Australian Privacy Principles and confirms our commitment to respect the privacy rights of families, (parent/students) employees, and all individuals in the workplace, and those interacting with the CE and our Schools.

This policy describes:

- who we collect information from;
- the types of personal information collected and held by us;
- how this information is collected and held;
- the purposes for which your personal information is collected and used;
- how we store your personal information;
- disclosure of your personal information, including to overseas recipients;
- how you can gain access to your personal information and seek its correction; and
- how you may complain or inquire about our collection, handling, use or disclosure of your personal information and how that complaint or inquiry

### Policy

---

#### **Who do we Collect Personal Information From?**

We collect personal information from students, parents, prospective parents, job applicants, staff, volunteers and others including contractors and visitors and others that come into contact with us.

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

#### **What Types of Personal Information Do We Collect?**

The kinds of personal information we collect is largely dependent upon whose information we are collecting and why we are collecting it, however in general terms the school may collect:

- Personal Information including names, addresses, other contact details; financial information, photographic images and attendance records.
- Sensitive Information (particularly in relation to student and parent records) including religious beliefs, country of birth, languages spoken at home, memberships, court orders and criminal records.

- Health Information (particularly in relation to student and parent records) including medical records, disabilities, counselling reports, nutrition and dietary requirements.

**How do we collect personal information?**

How we collect personal information will largely be dependent upon the information we are collecting.

Where possible we have attempted to standardise the collection of personal information. However, given the nature of our operations, we often also receive personal information by email, websites, letters, notes, 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.

We may also collect personal information from other people (e.g. a personal reference) or independent sources. We will only do so where it is not reasonable and practical to collect the information from you directly.

Sometimes we may be provided with your personal information without having sought it out “unsolicited information”. Where we collect unsolicited information we will only hold, use and/or disclose that information if we could otherwise do so had we collected it by normal means. If that unsolicited information could not have been collected by normal means then we will destroy or, permanently delete the information.

**How we use personal information**

We only use personal information 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 by you, or to which you have consented.

The purposes for which we use personal information includes but is not limited to:

- providing education, pastoral care, extra-curricular and health services;
- keeping parents informed as to school community matters;
- marketing, promotional and fundraising activities;
- supporting the activities of school
- to satisfy our legal obligations, with regard to duty of care and child protection obligations.
- the employment of staff;
- the engagement of volunteers.

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

We only collect sensitive information reasonably necessary for one or more of these functions or activities, if we have the consent of the individuals to whom the sensitive information relates.

If we do not have the relevant consent and a permitted health situation or permitted general situation does not exist, then we may still collect sensitive information provided it relates solely to individuals who have regular contact with the school in connection with our activities.

We will only use or disclose sensitive information for a secondary purpose if you would reasonably expect us to use or disclose the information and the secondary purpose is directly related to the primary purpose.

We do not use information for direct marketing purposes.

We do not use government related identifiers unless required.

### **Sharing of Information between related system schools**

The Privacy Act allows a system school, being legally related to each of the other schools conducted by the CEO, to share personal (but not sensitive) information with other schools in the CEO System. This allows schools to transfer information between schools as long as the information is being used for the original purpose.

### **Storage and Security of Personal Information**

We store personal information in a variety of formats including on databases, in hard copy files and on personal 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.

### **When we disclose personal information**

We only use personal information for the purposes for which it was given to us, or for purposes which are related (or directly related in the case of sensitive information) to one or more of our functions or activities.

We may disclose your personal information to government agencies, other parents, other schools, recipients of school publications, visiting teachers, counsellors and coaches, our service providers, agents, contractors, business partners and other recipients from time to time, only if one or more of the following apply:

- you have consented;
- you would reasonably expect us to use or disclose your personal information in this way;
- we are authorised or required to do so by law;
- disclosure will lessen or prevent a serious threat to the life, health or safety of an individual
- where another permitted general situation or permitted health situation exception applies;
- disclosure is reasonably necessary for a law enforcement related activity.

### **Personal Information of Students**

The Privacy Act does not differentiate between adults and children and does not specify an age after which individuals can make their own decisions with respect to their personal information.

The CEO respects every parent's right to make decisions concerning their child's education. A school will refer any requests for consent and notices in relation to the personal information of a student to the student's parents or guardians. A school will treat consent given by parents as consent given on behalf of the student, and notice to parents will act as notice given to the student. There will be occasions when access is denied, including where the 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 student.

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

### **Disclosure of personal information to overseas recipients**

We may disclose personal information to overseas recipients in certain circumstances, such as when we are organising an overseas excursion. 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); or
- We have satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime; or
- 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

### **How to gain access to your personal information we hold**

You may request access to the personal information we hold about you, or request that we change the personal information, by contacting us.

### **How we ensure the quality of personal information**

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up to date. These steps include ensuring that the personal information is accurate, complete and up to date at the time of collection and when using or disclosing the personal information. On an ongoing basis we maintain and update personal information when we are advised by individuals or when we become aware through other means that their personal information has changed.

### **Correction of personal Information**

To make a request to access or update any personal information the CEO or a System school holds about you or your child, contact the school's Principal in writing.

### **Privacy Complaints**

If you wish to make a complaint about a breach by us of the Australian Privacy Principles or the Health Privacy Principles you may do so by providing your written complaint by email, or letter or by personal delivery to any one of our contact details as noted below. You may also make a complaint verbally.

We will respond to your complaint within a reasonable time (usually no longer than 30 days) and we may seek further information from you in order to provide a full and complete response.

Your complaint may also be taken to the Office of the Australian Information Commissioner.

## Data Breaches and Privacy Breaches

What is a Notifiable Data Breach?

The Privacy Act refers to an “eligible data breach”, while the OAIC uses the term NDB on its website.

Under the Act a data breach must be notified where:

- there is unauthorised access to, or unauthorised disclosure of, personal information; and
- a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the personal information relates. OR Personal information is lost in circumstances where:
  - unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
  - assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

Further information on identifying an eligible data breach can be found on the Office of the Australian Information Commissioners website:

<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches>

## Serious Harm

Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the school’s position would identify as a possible outcome of the data breach.

## What to do when there is a Data or Privacy Breach

Where an eligible data breach is suspected or believed to have occurred a school must log a critical incident form containing a statement of prescribed information regarding an eligible data breach that is believed to have occurred.

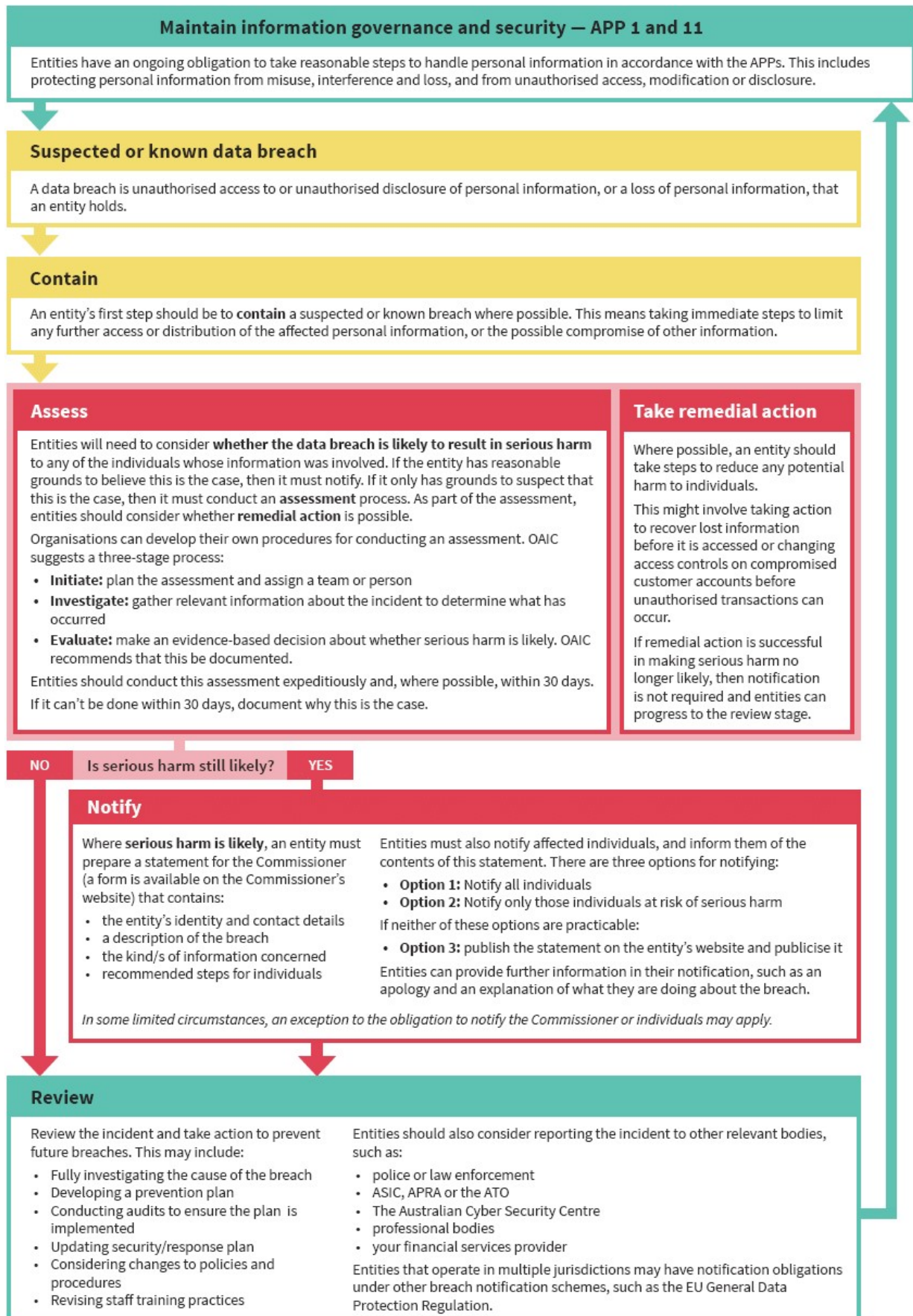
The Principal or CE Privacy Officer will in line with OAIC’s process for identifying an eligible data breach (<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches#preventing-serious-harm-with-remedial-action>)

then:

- Carry out a risk assessment in the event that an eligible data breach is suspected;
- Prepare a statement of prescribed information regarding an eligible data breach that is believed to have occurred (if appropriate);  
<https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB>
- Submit the statement to the OAIC (if appropriate); and
- Contact all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

We will take all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

This is summarized in the following diagram from the OAIC



## Definitions

---

### Personal information

Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- a) whether the information or opinion is true or not
- b) whether the information or opinion is recorded in a material form or not.

### Sensitive information:

- a) information or an opinion about an individual's:
  - i. racial or ethnic origin
  - ii. political opinions
  - iii. membership of a political association
  - iv. religious beliefs or affiliations
  - v. philosophical beliefs
  - vi. membership of a professional or trade association
  - vii. membership of a trade union
  - viii. sexual orientation or practices
  - ix. criminal record that is also personal information
- b) health information about an individual (including information about a disability or an Individual Learning Plan)
- c) genetic information about an individual that is not otherwise health information
- d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification
- e) biometric templates.

### 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.

### Record:

The Privacy Act regulates personal information contained in a 'record'. A 'record' includes a 'document', whether in paper form or held in an electronic or other device. The definition in the Amending Act is Privacy inclusive and therefore now covers a wide variety of material which might constitute a record. A 'document' is defined to include anything on which there is writing, anything from which sounds, images or writings can be reproduced, drawings or photographs.

---

## Summary of Relevant Australian Privacy Principles (APPs)

---

### **APP 1 — Open and transparent management of personal information:**

This principle ensures that the schools and the Catholic Education Office manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

### **APP 3 — Collection of solicited personal information:**

This principle outlines when schools and the Catholic Education Office can accumulate personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

### **APP 4 — Dealing with unsolicited personal information**

This principle outlines how schools and the Catholic Education Office must deal with unsolicited personal information.

### **APP 5 — Notification of the collection of personal information**

This principle outlines when and in what circumstances schools and the Catholic Education Office collects personal information, and when they must notify an individual of certain matters.

### **APP 6 — Use or disclosure of personal information**

This principle outlines the circumstances in which schools and the Catholic Education Office may use or disclose personal information that it holds.

### **APP 7 — Direct marketing**

This principle stipulates that an organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

### **APP 8 — Cross-border disclosure of personal information**

This principle outlines the steps schools and the Catholic Education Office must take to protect personal information before it is disclosed overseas.

### **APP 10 — Quality of personal information**

This Principle requires schools and the Catholic Education Office to take reasonable steps to ensure the personal information it collects is accurate, up to date and complete and relevant, having regard to the purpose of the use or disclosure.

### **APP 11 — Security of personal information**

This principle requires schools and the Catholic Education Office to take reasonable steps to protect personal information it holds from misuse, interference and loss, *and from unauthorised access*, Privacy modification or disclosure. An entity also has obligations to destroy or de-identify personal information in certain circumstances.

### **APP 12 — Access to personal information**

This principle outlines the obligations of schools and the Catholic Education Office when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.



**APP 13 — Correction of personal information**

This principle outlines the obligations of schools and the Catholic Education Office in relation to correcting the personal information it holds about individuals.

**Contact Us**

---

You can contact us about this Policy or about your personal information through contacting the CEO.

The CEO's contact details are:

Catholic Education Office  
PO Box 3317  
Manuka ACT 2603  
Phone: (02)6234 5455  
Email: [reception@cg.catholic.edu.au](mailto:reception@cg.catholic.edu.au)

If you are not satisfied with the CECG's decision you may make a complaint to the Office of the Australian Information Commissioner (OAIC) whose contact details are:

GPO Box 5218, Sydney, NSW 2001  
Telephone: 1300 363 992  
[www.oaic.gov.au](http://www.oaic.gov.au)

**Forms**

---

Standard Collection Notice for Schools  
Employee Collection Notice

Approved By:	Service Area Leadership Team	26 <sup>th</sup> November 2018
Policy Review Date:	August 2020	
TRIM Record Number:	R441300	