POLICY	PROCEDURE
Policy Name	Privacy Policy
NESA Policy Category	Staff (B3)
Related Procedures	Privacy Breach Checklist Privacy Breach Response Plan
Related Policies and Legislation	Privacy Act 1988 Privacy Amendment (Enhancing Privacy Protection) Act 2012 Privacy Amendment (Notifiable Data Breaches) Act 2017 Australian Privacy Principles Office of the Australian Information Commissioner (OAIC) – Data Breach Notification Guidelines
Date of Issue / Last Revision	*9 April 2019* *18 March 2022* *21 January 2026*
Date Set for Review	*January 2028*

Central Coast Montessori Primary School Privacy Policy

1. Introduction

Central Coast Montessori School acknowledges the weighty amount of personal information it collects, holds and manages, in order to provide its Educational Services to families who seek to enrol their children at the School. The School respects the confidentiality of this information and is careful to comply with Privacy legislation and the Australian Privacy Principles.

2. Scope

This policy applies to Students, Parents, Board members, Employees and Volunteers, employers, contractors, and people visiting the school site. This policy outlines how the School collects, uses and protects Personal Information. As well as how the School responds to complaints of breach of Privacy.

3. Legislation, Documentation & Policies

- Privacy Act 1988 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Australian Privacy Principles
- Office of the Australian Information Commissioner's (**OAIC**) Guide *Data Breach*

Notification: a guide to handling personal information security breaches

- Application Forms
- Admission/Enrolment Contract
- Student Protection Policies & Procedures
- Policies for students with Disabilities
- Other relevant School Policies

4. Definitions

Breach means unauthorized access and unauthorized disclosure of personal information of individuals including in circumstances where there has been a possible unauthorised access or disclosure which compromises personal data.

Eligible data refers to personal information of a (confidential) sensitive nature which could result in significant harm / damage or risk to those affected by a breach.

Examples of eligible data breaches include:

- Disclosures of Medical numbers or Financial Accounts;
- Disclosure of mental illness, disability, or home addresses of “protected people”.

The consequences of eligible data breaches can include:

- Threat to emotional wellbeing;
- Damage to reputation;
- Defamation.

Employee means all employees employed by the School, including applicants and prospective employees.

Employee Record means a record as defined in the Act. (Employment Records are exempt from Privacy protection.)

Health Information is a subset of sensitive information. It is information or an opinion about the health or disability of an individual and information collected to provide, or in providing a health service.

Health Service includes an activity performed to assess, record, maintain or improve an individual’s health, to diagnose an illness or disability, to treat an individual, or the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Mandatory Notification means that the School must notify the Australian Information Commissioner when an eligible breach has occurred.

Parent is the parent / guardian / carer of a student.

Personal information is information or an opinion, whether true or not, and whether recorded in material form or not, about an identified individual or an individual whose identity is reasonably apparent, or can be determined, from the relevant information or opinion.

Response Team is a small group of delegated staff whose role is to respond to alleged or

known breaches of personal information held by the school.

Response Plan means the Plan followed by the Response Team following an actual or suspected breach of data.

Sensitive information is a type of personal information. It includes 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 preference or practice, or criminal record. Sensitive information also includes biometric information that is used for the purpose of automated biometric verification, biometric identification or biometric templates.

Student means prospective, current or past student of the School.

5. What kind of personal information does the School collect and how does the School collect it?

The type of information the School collects and holds includes (but is not limited to) personal information, including sensitive information, about:

- Students and parents and/or guardians (hereinafter called "parents") before, during and after the course of a student's enrolment at the School;
- Job applicants, staff members, volunteers and contractors;
- Employee Candidates. If the person is a candidate seeking employment with the School, the School may collect and hold information about the candidate including the candidate's name, address, email address, contact telephone number, gender, age, employment history, references, resume, medical history, emergency contact information, taxation details, qualifications and payment details; and
- Other people who come into contact with the School.

Unsolicited information provided to the school by third parties will be destroyed unless required to be addressed by law.

6. Transparency and Process of Collection:

The School will generally collect personal information from parents and/or students by way of Forms, face-to-face meetings and interviews, and telephone calls. In some circumstances the School may be provided with personal information from a third party, for example, a report provided by a medical professional, a reference from another school, Family Court Order.

7. Employment Candidates and Exception in relation to Employee Records:

Under the Privacy Act and Principles, employee records are not protected from disclosure. Examples of Employee Records which are not covered (and about which information **can be properly shared** between employers) are:

- The engagement, training, disciplining or resignation of the employee/potential employee;
- The terms of any termination of the employment;
- The terms and conditions of the hiring/employment of the employee;
- The employee's personal and emergency contact details;
- The employee's performance or conduct issues, if any;
- The employee's hours of employment;
- The employee's salary or wages;
- The employee's membership of a professional or trade association;
- The employee's trade union membership;
- The employee's annual, long service, personal, parental or other leave;
- The employee's taxation, banking or superannuation affairs; or
- The employee's Health Information.

Note: A prospective new Employer must ASK the questions; there is no obligation for a previous employer to volunteer the information.

The exemption applies to current or former employees. It does not apply to contractors, volunteers or prospective employees.

8. Anonymity

The Privacy Principles provide the option for individuals not to identify themselves when entering into transactions with an organisation wherever this is lawful and practical. However, given the needs of schools to collect and use personal information for their educational purposes **ANONYMITY is not likely to be practical or even possible** for any number of reasons including the School's duty of care, insurance purposes, administration purposes, etc. Most "transactions" would require a person's details in some form.

Examples of where individuals would be able to remain anonymous would be:

- where an individual requests a School prospectus and it can be provided without collecting the individual's personal information (e.g. at a School Open Day); or
- where a survey is conducted and there is no need to collect a respondent's personal information such as their name and address.

9. Purpose of Collection

a) From Families

The **primary purpose** for which the School uses personal information (initially and on-going) is to assess and respond to the educational needs of students and fulfil relevant duties and obligations.

The secondary purposes related to the Primary Purpose include:

- Keeping Parents informed about matters related to their child's schooling, through correspondence, newsletters and magazines;
- Day-today administration;
- Looking after pupils' pastoral and medical wellbeing;
- Fee payment;
- Assessing hardship requests;
- Seeking donations and marketing for the School;
- Satisfying the School's legal obligations and discharging its duty of care.

Full and frank disclosure is a fundamental requirement without which the initial and/or ongoing enrolment of the student may be compromised.

b) From Job applicants, staff members and contractors:

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

The purposes for which the School uses personal information of job applicants, staff members and contractors include:

- In administering the individual's employment or contract, as the case may be;
- For insurance purposes;
- Seeking funds and marketing for the School;
- To satisfy the School's legal obligations, for example, in relation to child protection legislation.

c) From Volunteers:

The School also obtains personal information about volunteers who assist the School in its functions or conduct associated activities, (such as alumni associations), to enable the School and the volunteers to work together.

10. To whom might the School disclose Personal Information?

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

- Another school;
- Government departments;
- Medical practitioners;
- People providing services to the School, including specialist visiting teachers and sports coaches;
- Recipients of School publications, like newsletters and magazines;
- Parents; and
- Public Health, Safety or Police Authorities, including as mandated by law;
- Law Enforcement Authorities; and

- By consent or to anyone you authorise the School to disclose information to.

11. Sending Information Overseas

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.

The school may be disclose personal information to a reputable overseas entity such as a cloud-hosting service provider for the purposes of delivering educational and support services across the School.

Where student use of an online or cloud-based service requires parental consent, and the School deems the use of the service is appropriate for the provision of educational or administrative services, parental consent is implied by acceptance of this policy, (by continuing enrolment), in place of a separate signed parental consent for each of these individual services.

12. Overseas disclosure and cloud

The School may disclose personal information about an individual overseas; this is likely to occur if the School uses 'cloud' service providers.

When disclosing personal information, the School will take all steps reasonable to ensure that the overseas recipient complies with the Australian Privacy Principles.

13. How does the School treat sensitive information?

In referring to "sensitive information", the School 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, that is also personal information; and health information about an individual.

Sensitive information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless consent is given, or agreed to, or the use or disclosure of the sensitive information is allowed for legal purposes.

14. Marketing and Fundraising

For the purposes of marketing, the use of personal information can be considered but only with consent. The School treats marketing for the future growth and development of the School as an important part of

ensuring that the School continues to be an excellent learning environment in which both students and staff thrive.

Personal information held by the School may be disclosed to an organisation that assists in the School's fundraising, for example, the School's Foundation or alumni organisation.

Parents, staff, contractors and other members of the wider School community may from time to time receive fundraising information.

15. Management and Security of Personal Information

School employees are required to respect the confidentiality of students' and parents' personal information.

The School has in place reasonable steps to protect the personal information the School holds from misuse, loss, interference, unauthorised access, modification or disclosure.

The School will destroy or de-identify information when it is no longer needed or not subjected to Notice.

Hard Copy Files

Hard copy files are to be stored in locked storage, be it onsite or offsite. Access to these records is restricted to authorised School employees.

All authorised School employees must ensure that all papers and files relating to School Employees are stored in locked areas at night, when authorised employees are absent from the office or at other times when authorised employees are not working on such papers or files.

Any destruction of copies of documents or unwanted pieces should be by way of secure destruction bin or shredding.

Electronic Files

All electronic correspondence or other electronic documents regarding Personal Information are filed in the appropriate employee file in the School's document storage solution. Only authorised employees have access to these files. Authorised employees may only access electronic or hard copy files for known and the authorized purposes

Any person who accesses a file for an unauthorised purpose will be subject to disciplinary action, including where appropriate, dismissal.

16. Accuracy and Updating of Personal Information

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 Student Services Office of the School.

17. Access to Files

Parents may seek access to personal information held by the School about them or their children by contacting the School Principal. 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, or where the release may result in a breach of the School's duty of care to the student.

Students will generally have access to their personal information through their parents, but adult students (students 16 years and older) may seek access themselves.

To make a request to access any information the School holds about you, or your child, please contact the School Principal in writing.

The School may require you to verify your identity and specify what information you require. The School may charge a fee to cover the cost of verifying your application and locating, retrieving, reviewing and copying any material requested. If the information sought is extensive, the School will advise the likely cost in advance.

If a request for access is refused in accordance with the APPs, the School will provide written reasons why the request was refused. Details on how to make a complaint will also be included in this response.

The bases upon which access to records can be refused are as follows:

- In the case of Personal Information other than Health Information, that providing access would pose a serious and imminent threat to the life or health of any individual;
- In the case of Health Information, that providing access would pose a serious threat to the life or health of any individual;
- Providing access would have an unreasonable impact upon the privacy of other individuals;
- The request for access is frivolous or vexatious;
- The information relates to existing or anticipated legal proceedings between the School and the individual, and the information would not be accessible through the process of

discovery in those proceedings;
- Providing access would reveal the School's intentions in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- Providing access would be unlawful;
- Denying access is required or authorised by or under law (such as in relation to legally privileged information);
- Providing access would be likely to prejudice an investigation of possible unlawful activity;
- Providing access would be likely to prejudice:
    - The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
    - The enforcement of laws relating to the confiscation of the proceeds of crime;
    - The protection of the public revenue;
    - The prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
    - The preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders.

18. Archived Materials

Personal information is stored in hard copy and electronically.
The Australian Privacy Principles do not state any specific time that records are to be archived. They simply provide that a school is not required to store personal information longer than "necessary for its purposes".

It is School policy to maintain complete student files and employee records for a reasonable time following the student's departure from the school. This is done to protect the interests of both the School and the relevant individual in terms of enquiries or allegations that may be made at any time in the future. The School reserves the right to charge a fee for access to non-current enrolments or employment as outlined above.

Hardcopy Tax File Number (TFN) Declarations

Where the School receives completed hard copy TFN Declaration Forms, the Tax File Number must be "blacked" out once the details have been entered into the payroll system. The Form should then be placed in the employee's personnel file.

Electronic Tax File Number (TFN) Declarations

Where Employees submit their TFN Declaration electronically, the record is contained electronically in the organisation's document storage solution. Only authorised employees have access to these files.

19. Archiving and Destruction

Unless subject to a relevant Notice, the School is required to keep time and wages records for its employees for seven years.

Privacy legislation does not state how long archives of personal information are to be kept.

20. Data Breaches and Mandatory Notification to the Office of the Australian Information Commissioner (OAIC)

A Notifiable Data Breach occurs when Personal Information of an individual held by the School is accessed by, or is disclosed to, an unauthorised person, or is lost, and:

- a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual; or
- in the case of loss (eg leaving a laptop containing Personal Information on a bus);
- unauthorised access or disclosure of Personal Information is likely to occur, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual.

21. Response Plan/Process for known or Alleged Breach of Privacy.

If the School knows or reasonably suspects that a Data Breach of Privacy has occurred,

- It will call together the Response Team;
- The Response Team will activate the 4-Step Response Plan/Process;
- See Annexure D
- The Response Team will conduct a reasonable and expeditious **initial assessment** to determine the nature and extent of the breach and if there are reasonable grounds to believe that a Notifiable Data Breach has occurred;
- It will take all reasonable steps to ensure that a full assessment is completed within 30 days of becoming aware of the suspected Notifiable Data Breach.

22. Notification

Subject to any restriction under the Act, in the event a Notifiable Data Breach occurs, the School will, as soon as practicable, prepare a statement outlining details of the breach, and:

- notify the individual of the unauthorised access, disclosure or breach; and
- notify the Office of the Australian Information Commissioner of the unauthorised access, disclosure or breach.
- See Annexure C

23. Complaints Process

If an individual believes that the School has breached the APPs a complaint can be made to the School.

All complaints should be in writing and directed to the Principal / Privacy Officer. The School will investigate complaints in a timely manner and respond in writing.

If an individual is not satisfied with the School's response, a complaint can be lodged with the Office of the Australian Information Commissioner on the following website http://www.oaic.gov.au/privacy/making-a-privacy-complaint.

The School also allows individuals to "opt out" through selection on the Standard Collection Notice, or on the enrolment agreement.

24. Review

This policy will be updated bi-annually or as necessitated by law.

Annexures A, B, C, and D are attached.

*Privacy Annexure A: Alumni Privacy Collection Notice
*Privacy Annexure B: Notification of 'Eligible Breach' to the Office of the Information Commissioner (OAIC) 2018
*Privacy Annexure C: Privacy Breach Checklist
*Privacy Annexure D: Privacy Breach Response Plan

Annexure A

Alumni Privacy Collection Notice

1. The school may collect personal information about you for the purpose of:
   Providing up to date information about activities of the Association and its members highlighting, as appropriate, historical events and achievements of the school and its past pupils and to keep alumni members informed about other members.

2. The information must be provided to ensure continuing and meaningful membership.

3. We also, from time to time engage in fundraising activities. The information received from you may be used by the school to assist in its fundraising activities and also may be used to make an appeal to you for donations. If you do not agree to this, please advise us now.

   ⬜ I agree ⬜ I do not agree

4. The school may publish details about you in school publications and website. If you do not agree to this, you please advise us now.

   ⬜ I agree ⬜ I do not agree

5. The School's Privacy Policy, accessible on the School's website, contains details of how you may seek access to and correction of your personal information which the School has collected and holds, and how you may complain about a breach of the Australian Privacy Principles.

6. The 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 email services. 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 reside on a cloud service provider's servers which may be situated outside Australia. Further information about the School's use of on online or 'cloud' service providers is contained in the School's Privacy Policy. *

7. It may be the case that you can give the school details of other potential members/members. If you provide us with the personal information of others, we encourage you to inform them that you are disclosing that information to the School and why.

Name of Applicant/Member: _____

(Print)

Signature: _____ Date: _____

Annexure B

Notification Statement of "Eligible Breach" to the Office of the Information Commissioner (OAIC) 2018

Used for Mandatory Reporting to Privacy Commissioner

(where there is a risk of serious harm to individuals or school arising from Privacy Breach)

Contact Details of School: _____

_____

Details of the **Eligible Breach** (significant harm): _____

_____

_____

Nature of possible serious harm: _____

_____

_____

Remedial/mitigation action taken: _____

_____

_____

Who are the likely affected individuals? _____

_____

How many individuals may be affected? _____

Is notification to individuals sufficient or is the school making a public notification via website or social media?

_____

_____

Future Actions: _____

_____

Date: _____ Email for Commissioner is enquiries@oaic.gov.au

Annexure C

Privacy Breach Checklist

Form: Breach Checklist for Response Team (Evaluation and Mitigation)
(To be used for a preliminary assessment of level of risk (High, Medium or Low) arising from breach.)

Date Breach occurred: _____

Date breach reported: _____

Date of Completion of Checklist: _____

The Response Team has followed the following steps:

- ⬜ identified the type of personal information involved in the Privacy Breach;
- ⬜ identified the date, time, duration, and location of the Privacy Breach;
- ⬜ established the extent of the Privacy Breach (**number** of **individuals** affected);
- ⬜ considered what mitigation actions are appropriate in the short term;
- ⬜ considered what mitigation actions are appropriate in the long term;
- ⬜ established **who** the affected, or possibly affected, individuals are;
- ⬜ assessed whether there needs to be a "public" notification using social media (in addition to contacting individuals who are affected);
- ⬜ reached a preliminary assessment of breach:
  - ⬜ High
  - ⬜ Medium
  - ⬜ Low
- ⬜ Proceeded in accordance with the assessment level;
- ⬜ Entered a record of the breach in the Breach Log.

Name: Principal/Delegate for the Response Team: _____

Signature of Principal/Delegate for the Response Team: _____

Date: _____

Annexure D

Privacy Breach Response Plan

Response Plan (required by legislative changes to Privacy Law effective from 22 02 2018

The Australian Information Commissioner advises the importance of keeping **appropriate records** of responses to Privacy Breaches, by way of transparent and consistent use of a **Response Plan.** The Response Plan will include the assessments of the risks associated with the Privacy Breach and decisions made as to the appropriate action/s to take in response to the Privacy Breach.

The Response Plan is a 4-Phase Process.

In the event of a Privacy Breach, School personnel **must adhere** to the following four phase process (as described in the Office of the Australian Information Commissioner's (OAIC) guide. *Data breach notification: a guide to handling personal information security breaches).* Phases 1 – 3 should occur in quick succession and may occur simultaneously.

Phase 1

Contain the Privacy Breach and do a preliminary assessment.

School personnel who become aware of the Privacy Breach must immediately notify the Principal or delegate who will inform the Response Team.

This notification should include (if known at this stage) the time and date the suspected Privacy Breach was discovered, the type of personal information involved, the cause and extent of the Privacy Breach, and who may be affected by the Privacy Breach.

The Principal/delegate and Response Team **must take immediate available steps** to contain the Privacy Breach (eg contact the IT department, if practicable, to shut down relevant systems or remove access to the systems).

In containing the Privacy Breach, **evidence** should be preserved that may be valuable in determining the cause of the Privacy Breach. This is particularly relevant if there is a Privacy Breach involving information security.

The Principal/delegate and Response Team delegate **must consider** if there are any other steps that can be taken immediately to mitigate the harm any individuals may suffer from the Privacy Breach.

The Principal/Delegate and Response Team must make a **preliminary assessment** of the risk level of the Privacy Breach. This will involve an analysis of the risks involved:

- ⬜ High
- ⬜ Medium
- ⬜ Low

Where a High-Risk incident is identified, it falls into the category of an eligible breach (mandatory reporting) and it must be treated as such by the Principal (and Response Team).

They **must consider** if the affected individuals should be notified immediately to mitigate the risk of serious harm to the individuals. The breach must also be reported to the Office of the Australian Information Commissioner within 30 days.

If the breach is identified as a **Medium Risk** and is reasonably considered to be an "eligible" breach (mandatory reporting) a notification must be made to the Commission – see Annexure Form.

If the breach is considered **Low Risk, Phases 2 and 3 below must be followed.**

<u>Phase 2</u>

Evaluation and Mitigation of the risks associated with the Privacy Breach (assessed as High, Medium or Low).

The Response Team is required to take **further steps** available (i.e. additional to those identified in Phase 1) to contain the Privacy Breach and mitigate harm to affected individuals by:

- ⬜ identifying the type of personal information involved in the Privacy Breach;
- ⬜ identifying the date, time, duration, and location of the Privacy Breach;
- ⬜ establishing the extent of the Privacy Breach **(number** of **individuals** affected);
- ⬜ establishing **who** the affected, or possibly affected, individuals are;
- ⬜ assessing whether there needs to be a "public" notification using social media;
- ⬜ identifying what is the risk of harm to the individual/s and the extent of the likely harm (eg what was the nature of the personal information involved);
- ⬜ assessing the risk of harm to the school;

- ⬜ establishing what the likely **reoccurrence** of the Privacy Breach is;
- ⬜ considering whether the Privacy Breach indicates a **systemic problem** with practices or procedures; and
- ⬜ establishing the likely cause of the Privacy Breach.

Phase 3

Privacy Breach Notifications

It is the responsibility of the Response Team to determine whether to notify the following stake holders of the Privacy Breach.

- Affected individuals
- Parents
- The Privacy Commissioner, and/or
- Other stakeholders (other entities who may share the information).

The main consideration before choosing what action to take is to ask:

"Does this breach raise a **real risk of serious harm** to affected individuals or the school?"

The Response Team

- **The Response Team needs to be chosen to reflect their skills and their authority to take action when there is a breach of Privacy.**
- **All staff must be aware of their responsibility to inform the Team of a breach.**
- **Each person on the Response Team needs to know what action he/she is responsible for when there is a breach.**

Role	Responsibilities and Authority for...	First person to Contact?	Second person to Contact?
Principal			
IT			
HR			
Legal			
Other			

Other			

The **Investigation of the breach** will be guided by:

- the Response Plan and
- the School Formal Complaints Policy

Phase 4

Action to prevent future Privacy Breaches

Additional to following the Response Plan and Formal Complaints Policy, details of:

- the Breach and
- the Cause and
- the Outcome

must be recorded in a **Privacy Breach Log**.

The Principal must review the Breach Log annually, to identify any recurring breaches.

All Staff must be trained in Privacy Principles and Awareness of the confidentiality of the copious personal and sensitive information available to them and accessible to them and that breaching privacy is an offence.

Staff in positions of managing copious amounts of personal and sensitive information (Bursars, PA's, IT personnel) must be made aware of their special responsibility and that breaching of privacy is now considered an offence which MUST frequently be reported to the Privacy Commissioner.

Useful contacts

National Computer Emergency Response Team (CERT) Report Privacy Breaches to CERT via email (info@cert.gov.au) or telephone (1300 172 499). Office of the Australian Information Commissioner (OAIC) Report Privacy Breaches to OAIC via email (enquires@oaic.gov.au) or telephone (1300 363 992).

Date signed: _____