

POLICY		PROCEDURE
Procedure Name	ICT, Social Media and Technology Use Procedure	
NESA Manual Section	School Management and Operation (B2) Schools Must be Maintained through Proper Governance (B2.3)	
Related Procedures & Registers	Code of Conduct for Staff Procedure (B2.3) Communication Procedure (B2.3) Complaint Handling Procedure (B8.2) Complaint Handling Procedural Fairness Guidelines (B8.2) Child Protection Procedure (B8.1) Document and Record Retention Procedure (B2.3) Student Academic Integrity Procedure (B4.1) Work Health and Safety Procedure (B2.3) Privacy, Personal Information and Confidentiality Procedure (B2.3)	
Related Policies	ICT, Social Media and Technology Use Policy (B2.3) Code of Conduct for Staff Policy (B2.3) Communication Policy (B2.3) Complaint Handling Policy (B8.2) Child Protection Policy (B8.1) Document and Record Retention Policy (B2.3) Student Academic Integrity Policy (B4.1) Work Health and Safety Policy (B2.3) Privacy, Personal Information and Confidentiality Policy (B2.3)	
Related Legislation	Privacy Act 1988 (Cth) Work Health and Safety Act 2011 (NSW) Education Act 1990 Copyright Act 1968 (Cth)	
Date of Issue / Last Revision	21 January 2020 18 March 2022 04 December 2025 1 May 2026 22 August 2026	
Date Set for Review	August 2029	

ICT, Social Media and Technology Use Procedure

Central Coast Montessori Primary School Ltd (CCMPS) implements practical procedures to ensure the safe, secure, professional and effective use of technology resources, communication systems, digital platforms and social media.

This procedure outlines day-to-day requirements for access, use, supervision, security, communication, equipment management and incident response.

Scope

This procedure applies to all staff, contractors, volunteers and other authorised users of School technology resources.

Relevant sections also apply to students when using School technology under supervision, and to personal device use where it impacts School operations or the School community.

Key Principles

- Security first – systems and data must be protected.
- Professional use – technology must be used respectfully and responsibly.
- Child-safe practice – online conduct must protect students and maintain boundaries.
- Operational efficiency – School resources should support educational and business purposes.
- Accountability – users are responsible for actions taken using School systems.
- Prompt reporting – issues and incidents must be reported quickly.

Content / Procedural Steps Taken

Access to Systems and Accounts

Access to School systems, email accounts, shared drives, learning platforms and devices is granted according to role requirements and authorised by the Principal or delegate.

Users must:

- use only their allocated accounts and credentials
- keep passwords confidential
- not share logins without approval
- log out of shared or unattended devices
- notify the School when access issues arise.

Access may be changed or removed when duties change or employment ends.

Passwords and Security Controls

Users must take reasonable steps to protect access credentials and systems. This includes:

- using strong passwords
- changing passwords when directed or when compromise is suspected
- not writing passwords in unsecured locations
- enabling additional security controls where provided
- locking screens when devices are unattended.

Use of School Devices and Equipment

School devices, telephones, printers, peripherals and other equipment are provided primarily for School purposes. Users must:

- take reasonable care of equipment
- use equipment safely and lawfully
- not intentionally damage or misuse equipment
- report faults, loss or damage promptly
- return equipment when requested or on cessation of employment.

Unauthorised removal of equipment from site is not permitted unless approved.

Email, Internet and Communication Use

School email, internet and communication systems must be used professionally and appropriately. Users must not:

- send offensive, abusive or misleading messages
- access inappropriate or unlawful material
- use systems for harassment or bullying
- subscribe the School to unnecessary services
- engage in excessive personal use during work time.

Users should exercise care before opening links, attachments or unexpected messages.

Social Media and Public Online Activity

Where the School, staff, students or families may be identified, users must behave professionally and responsibly online.

Users must not:

- publish confidential information
- post images of students without approval
- make defamatory or inappropriate comments
- present personal opinions as those of the School
- engage in conduct likely to damage the School's reputation or workplace relationships.

Staff should make clear when views are personal and not those of the School.

Communication with Students and Families

Digital communication with students and families must occur through approved School platforms or authorised channels.

Communication must be:

- professional
- respectful
- relevant to School matters
- transparent and capable of oversight
- appropriately timed.

Private messaging, hidden communication channels or informal personal contact with students is not permitted.

Broader requirements relating to School communication, communication channels, recordkeeping and escalation are addressed in the *Communication Policy and Procedure*.

Student Use of Technology

Where students use technology, staff are responsible for appropriate supervision and guidance. Staff should:

- provide clear expectations for safe and respectful use
- supervise internet and device use appropriate to age
- support digital citizenship
- respond to misuse promptly
- report significant concerns to leadership.

Student learning use should also align with the Student Academic Integrity Policy where relevant.

Use of Personal Devices

Limited use of personal devices may occur where appropriate. Personal devices used for School purposes must not compromise privacy, security or professional boundaries.

Users must not store sensitive School information on personal devices unless authorised and appropriately secured.

Privacy, Confidentiality and Records

Users must protect personal information, confidential records and School data. This includes:

- accessing information only where authorised
- sharing information only on a need-to-know basis
- securely storing electronic records
- using approved systems where available
- following retention and disposal requirements.

Artificial Intelligence and Emerging Technology

Artificial intelligence (AI) and emerging technologies may be used for teaching, learning, administration and School operations where their use is appropriate, authorised and consistent with School requirements.

When using AI or emerging technologies, employees must:

- use only tools and platforms that are appropriate for the intended School purpose;
- not enter confidential, sensitive or personal information relating to students, families, employees or School operations into unauthorised AI platforms;
- exercise professional judgement and retain responsibility for work produced or supported by AI;
- review AI-generated content for accuracy, appropriateness, bias and reliability before using, sharing or relying upon it;
- verify important factual information rather than relying solely on AI-generated content;
- consider copyright, intellectual property, attribution and privacy requirements when creating or using AI-generated material;
- ensure AI use does not replace professional judgement, appropriate human oversight or required decision-making processes;
- follow any School guidance regarding approved platforms, appropriate use and information security; and
- undertake relevant guidance or training provided by the School as AI use and associated risks develop.

Student Use of AI

Student access to and use of AI must be age-appropriate, educationally purposeful and appropriately supervised.

Where AI is used as part of teaching and learning, employees must:

- clearly explain when and how students may use AI;
- ensure students understand when AI use is not permitted;
- establish appropriate expectations for acknowledging or disclosing AI assistance;
- support students to understand that AI-generated information may be inaccurate, incomplete or biased;
- encourage students to critically evaluate AI-generated information rather than accepting it as authoritative;
- ensure AI use supports, rather than replaces, students' own thinking, creativity and demonstration of learning;
- consider academic integrity when designing or assessing student work; and
- provide appropriate supervision and guidance having regard to students' age, maturity and learning needs.

Students must not enter personal, sensitive or confidential information about themselves or others into AI platforms unless specifically authorised and appropriately supervised by the School.

Monitoring and Review of AI Use

The School will periodically review its use of AI and emerging technologies having regard to educational value, staff and student experience, privacy and information security, academic integrity, emerging risks and developments in relevant guidance.

AI-related guidance and practices may be updated as technologies, educational applications and associated risks evolve.

Monitoring and System Administration

School-owned devices, accounts and networks may be monitored, maintained, audited or reviewed for operational, legal, safety or security purposes, to the extent permitted by law.

Reporting Incidents or Misuse

Users must promptly report concerns such as:

- suspected cyber incidents
- phishing emails
- lost or stolen devices
- privacy breaches
- inappropriate online conduct
- unauthorised access
- significant equipment damage or malfunction
- inappropriate or unauthorised use of AI or emerging technologies.

Reports should be made to the Principal or delegated staff member as soon as practicable.

Breaches and Corrective Action

Where misuse or breaches occur, the School may respond through:

- guidance or re-training
- restriction of access

- recovery of equipment
- formal management action
- disciplinary processes
- referral to external authorities where required.

Responses will be proportionate to the circumstances.

Record Keeping

The School may retain records relating to:

- issued devices or equipment
- access permissions
- incidents or breaches
- investigations
- acknowledgements or training
- repairs or replacements
- communication records where relevant.

Records must be stored securely.

Continuous Improvement

The School may periodically review technology use practices to improve:

- cybersecurity readiness
- staff awareness
- system efficiency
- child-safe digital practices
- communication systems
- emerging technology governance.

Monitoring, Evaluating and Review

Annual adjustments may be made to this procedure in response to identified areas for improvement to ensure it remains current, effective and aligned with School practice. Otherwise, this procedure will be reviewed every three (3) years, or earlier if required due to changes in legislation, technology risks, NESA requirements or identified gaps in practice.

Continuous improvement will be guided by cyber risk developments, legislative change, best practice and operational review.

Related Documents and References

[Child Safe Standards \(NSW\)](#)

[Independent Schools NSW Governance Resource Manual March 2026](#)

[Independent Schools NSW Workplace Management Social Networking Guidance](#)

[Independent Schools NSW – AI Implementation Framework for Schools \(2026\)](#)

[NESA Registered and Accredited Individual Non-Government Schools \(NSW\) Manual February 2026](#)

[NESA Resources for Schools](#)

In the event of any inconsistency between this Procedure and applicable legislation, the legislation will prevail.