

POLICY		PROCEDURE
Policy Name	ICT, Social Media and Technology Use Policy	
NESA Manual Section	School Management and Operation (B2) Schools Must be Maintained through Proper Governance (B2.3)	
Related Procedures & Registers	ICT, Social Media and Technology Use Procedure (B2.3) Communication Procedure (B2.3) Code of Conduct for Staff 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	Communication Policy (B2.3) Code of Conduct for Staff 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 Policy

Policy Statement

Central Coast Montessori Primary School Ltd (CCMPS) is committed to the safe, responsible, professional and lawful use of information and communication technology, digital systems, social media and emerging technologies.

Technology supports teaching, learning, communication, administration and operational efficiency. CCMPS expects all users of School technology resources and online platforms to act responsibly, maintain confidentiality, protect privacy and uphold the reputation of the School.

Use of technology must be consistent with the School's values, child-safe obligations, professional standards and legal responsibilities.

Purpose

This Policy establishes expectations for the use of School technology resources, digital systems, devices, communication tools, internet services, social media platforms and emerging technologies.

It provides a framework to manage cyber, privacy, conduct and reputational risks while supporting effective educational and operational use of technology.

Scope

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

Relevant sections also apply to students where technology use occurs under School supervision, and to personal technology use where it affects the School, students, staff or the School community.

Principles

Technology use at CCMPS is guided by the following principles:

- Safety – technology must support child safety, personal safety and cyber safety.
- Professionalism – digital conduct must reflect professional standards and respectful behaviour.
- Privacy and confidentiality – information must be protected and used appropriately.
- Security – systems and devices must be used in ways that reduce cyber risk.
- Responsible use – School resources must be used primarily for legitimate School purposes.
- Reputation – online conduct must not damage the School or members of the School community.
- Compliance – users must comply with laws, policies and reasonable directions.

Acceptable Use of Technology

Authorised users may use School technology resources for legitimate educational, administrative and operational purposes. Limited personal use may be permitted where it is reasonable, lawful, does not interfere with duties, does not incur unreasonable cost, and does not breach this Policy.

Use must not compromise system security, productivity, confidentiality or the School's reputation.

Unacceptable Use

Unacceptable use may include, but is not limited to:

- accessing, creating, storing or sharing offensive, illegal or inappropriate material
- bullying, harassment, discrimination or abusive conduct online
- unauthorised disclosure of confidential information
- unauthorised access to accounts, files or systems

- excessive personal use during work time
- downloading unapproved software or applications
- misuse of School devices, telephones or equipment
- infringement of copyright or intellectual property rights
- using technology to misrepresent identity or deceive others
- any use inconsistent with child-safe obligations.

Social Media and Online Conduct

All users must act responsibly when using social media or participating in online forums where the School, staff, students or families may be identified.

Users must not:

- make offensive, defamatory or misleading statements
- disclose confidential or personal information
- represent personal views as those of the School without authorisation
- publish images or information relating to students without approval
- post content that harms professional relationships or the School's reputation
- engage in online conduct likely to damage trust and confidence in employment relationships
- engage in inappropriate online interaction with students.

Where views are expressed in a personal capacity, users should make clear that those views are personal and do not represent the School.

Staff must maintain professional boundaries in all online communication.

Communication with Students and Families

Digital communication with students and families must occur through approved School channels unless otherwise authorised. Communication should be professional, appropriate, transparent and capable of oversight.

Private, secretive or informal communication channels with students are not permitted.

Broader requirements for communication with students and families are addressed in the *Communication Policy and Procedure*.

Privacy, Confidentiality and Records

Users must protect personal information, confidential records and School data. Information must only be accessed, used or shared where authorised and necessary.

School-related digital records may constitute official records and must be managed in accordance with record retention requirements.

Cybersecurity and System Protection

Users must take reasonable steps to protect School systems and data, including:

- using secure passwords
- maintaining device security

- reporting suspicious emails or cyber incidents
- following access controls
- using approved software and platforms
- taking care when handling sensitive information.

Use of Artificial Intelligence and Emerging Technology

CCMPS supports the thoughtful, ethical and age-appropriate use of artificial intelligence (AI) and emerging technologies where they support teaching, learning, administration or School operations.

AI must be used lawfully, ethically and appropriately, with human judgement and accountability retained for decisions and outputs. Use must be consistent with privacy, confidentiality, intellectual property, child safety and academic integrity requirements.

Personal, sensitive or confidential School information must not be entered into unauthorised AI platforms. AI-generated information must be appropriately reviewed for accuracy, suitability and potential bias before being relied upon or used for School purposes.

Student use of AI must be age-appropriate, educationally purposeful and appropriately supervised. Expectations regarding permitted AI use and disclosure must be made clear where AI may be used in student learning or assessment.

Monitoring and No Expectation of Absolute Privacy

To the extent permitted by law, School-owned systems, devices, networks and accounts may be monitored, accessed, audited or reviewed for operational, security, legal or compliance purposes. Users should not assume absolute privacy when using School resources.

Breaches of this Policy

Suspected breaches may be investigated and managed in accordance with relevant School policies and procedures. Outcomes may include education, restriction of access, disciplinary action or referral to external authorities where required.

Roles and Responsibilities

Principal

- Ensure implementation of this Policy
- Oversee technology governance and risk management
- Determine responses to serious breaches
- Support appropriate resourcing and controls

Administration Manager / Delegated ICT

- Support system administration and security controls
- Assist with user access and incident response
- Maintain operational records where relevant

Staff

- Use technology responsibly and professionally

- Protect privacy and confidentiality
- Follow School requirements and report concerns
- Maintain professional online boundaries

Students

- Use technology appropriately under supervision
- Follow staff directions and behavioural expectations

All Users

- Comply with this Policy and lawful directions relating to technology use

Monitoring, Evaluating and Review

Annual adjustments may be made to this Policy in response to identified areas for improvement to ensure it remains current, effective and aligned with School practice. Otherwise, this Policy 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](#)

[NSW Education Standards Authority Act 2013 \(NSW\)](#)

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