Early
Childhood
Management
Services

1.0
Corporate Services

Acceptable Use of IT and Online Safety Policy

Purpose

The Acceptable Use and Online Safety Policy establishes clear, organisation-wide expectations for responsible, respectful, lawful, and secure use of ECMS's information and communication technology (ICT) systems, devices, and digital services.

It applies to all users of ECMS digital resources and promotes a safe and productive environment where technology supports ECMS's work with children, families, and the broader community.

The policy aims to:

- Ensure that technology is always pedagogically led and safeguards the rights, safety and wellbeing of all children.
- Protect ECMS, its people and stakeholders from harm, legal risk, reputational damage, and breaches of trust arising from inappropriate or unsafe technology use.
- Ensures ICT use aligns with ECMS's operational and strategic goals.
- Safeguard ECMS's systems and information from misuse, compromise, or damage.
- Maintain a child-safe digital environment in compliance with the Education and Care Services National Regulations 2011 (Cth), the National Quality Standards (NQS) and the Child Safe Standards.

This policy is supported by practical guidelines to help users comply with procedures that define how access is managed, monitored, and governed.

Scope

This policy applies to:

- ECMS Board, Executive Leadership Team and Support Services.
- All ECMS-operated Early Learning Centres and Kindergarten programs.
- All ECMS employees, contractors, students on placement and volunteers.
- All families, parents/guardians/authorised persons enrolled in ECMS services, including during offsite excursions and activities.
- All ICT systems, networks, devices, services, applications, and data—regardless of whether access occurs from an ECMS site, remotely, or via personal devices.

Policy Statement

This policy outlines the expectations for the safe, responsible, and appropriate use of digital technologies, electronic equipment, and internet services across ECMS services, programs and activities. It aims to protect the wellbeing, privacy, and safety of all children, educators, families, and staff by promoting safe online practices and ensuring all equipment is used in a manner that supports educational outcomes and aligns with our duty of care under relevant legislation and standards, including the National Quality Framework and the Child Safe Standards (Vic). This policy applies to all individuals who access or use ECMS's digital resources.

Policy Principles

ECMS is committed to an anti-bias approach in early childhood. ECMS operates within a framework of social justice and equity - this means we celebrate family and cultural diversity and aim to be supportive, responsive, and inclusive of all children. This policy is underpinned by the principles of child safety, respect, responsibility, and inclusion. It recognises the importance of guiding young children in the safe and positive use of technology, while ensuring that all digital and electronic equipment is used ethically and for educational purposes. The policy supports compliance with the National Quality Standard, Early Years Learning Framework, and the Victorian Child Safe Standards. It promotes a shared responsibility among educators, staff, students on placement, contractors, children, families, and visitors in maintaining a secure and respectful digital environment. The rights to privacy, protection from harm, and equitable access to technology are central to these principles.

- **Appropriate Use of ICT Systems**

All users must use ECMS' ICT systems, devices and services in a lawful, ethical, and respectful manner that supports the organisation's values, mission, and daily operations.

- **Respectful and Responsible Behaviour**

Users must demonstrate integrity, accountability, and professionalism in all digital communications and interactions, whether internal or external. ICT systems must not be used to harass, bully, vilify, or threaten others.

- **Safe and Secure Technology Practices**

Users must take reasonable care to protect ECMS's ICT systems and data. This includes maintaining the confidentiality of login credentials, preventing unauthorised access, and reporting suspected security breaches or inappropriate content.

- **Use of Mobile Devices**

Mobile devices must be used only for authorised, work-related purposes, kept secure to prevent unauthorised access, and used with children only in age-appropriate, supervised ways that enhance—rather than replace—face-to-face interaction. All use must comply with ECMS policies on privacy, confidentiality, use of images, and data protection.

- **Pedagogically-led Technology**

Technology is used only when it meaningfully enhances children's learning, relationships, and wellbeing, not as a replacement for teacher/educator–child interactions.

- **Evidence-informed Practice**

While digital tools and Artificial Intelligence hold potential in ECE, ECMS acknowledges that evidence for their use is emerging. We commit to critical reflection, cautious adoption, and teacher/educator oversight in all applications.

- **Use of Personal Devices (BYOD)**

Personal devices are not used for ECMS work purposes including accessing ECMS systems or data. Staff will ensure mobile devices are not taken into the classroom other than for approved purposes. Personal devices cannot be used to take images of children.

Use of personal medical devices that require access to a personal device is permitted after informing the direct line manager.

- **Approved Use of Digital Devices – Staff Register**

In recognition of individual staff needs, ECMS permits the use of personal digital devices during work hours in specific, approved circumstances, such as for medical or health-related purposes. To ensure transparency and consistency, a staff register will be maintained at the service level to record all approved instances of device usage. Staff members seeking approval must submit a formal request outlining the reason for device use, supported by appropriate documentation where applicable (e.g., medical certificate). Each request will be assessed on a case-by-case basis by the direct line manager or designated approver, and written confirmation of approval will be recorded in the register. Approved staff are required to adhere to any conditions set out as part of the approval and must ensure device use is limited strictly to the permitted purpose.

Acceptable Use of Equipment

Reasonable Personal Use

Reasonable personal use of ECMS ICT systems is permitted if it does not interfere with work responsibilities, consume excessive resources, breach organisational policy, or expose ECMS to risk.

Prohibited Conduct

Users must not use ECMS ICT systems to engage in illegal activity, access or share offensive material, infringe intellectual property rights, or install unauthorised software or services.

Online Safety and Child Protection

ECMS is committed to fostering a safe, respectful, and inclusive online environment for all children, families, educators, and staff. The use of digital technologies, devices, and ICT systems within our services must support the safety, wellbeing, and development of every child. All use of ICT must comply with ECMS's legal and ethical obligations under the Child Wellbeing and Safety Act 2005 (Vic), the Children, Youth and Families Act 2005 (Vic), the Privact Act 1998 (Cth), the Privacy and Data Protection Act 2014 (Vic), and align with the Child Safe Standards (Vic) and the National Quality Standard (NQS). We promote responsible use of technology that protects children's rights, respects personal privacy, and supports positive learning experiences in early childhood settings.

Children are intentionally supported by teaching teams to develop early digital literacy skills such as privacy awareness, safe sharing, and respectful interactions, embedded within play-based pedagogy and aligned to the VEYLDF and EYLF v2.0. Families and caregivers receive transparent communication about the digital tools, platforms, or AI/Gen AI systems used in ECMS services.

To comply with these obligations:

Images – Video and Audio of Children

- Written parental/guardian consent is required before capture, storage, use of sharing.
- Personal devices must not be used to capture images or recordings of children.
- Files must be securely stored, accessed only by authorised personnel and destroyed in accordance with ECMS's retention schedule.
- For further information, refer to the *Use of Images of Children Procedure*.
- ECMS acknowledges that Aboriginal and Torres Strait Islander perspectives on image use, including the cultural significance and sensitivities around photographs, video and audio recordings. We commit to seeking guidance where appropriate and respecting community preferences regarding how images of Aboriginal children are stored, created and shared.
- Consent can be withdrawn at any time by the parent/carer in writing.
- Visitors, contractors and other adults are not permitted to take photos, video or audio recordings of children unless prior written consent has been obtained from parents/carers and authorised by the service.

Children's Safe Use of Digital Devices and Internet Access

- Children's access to digital devices and online content is always supervised and developmentally appropriate.
- Staff use co-viewing and guided use approaches to ensure technology is purposeful and supports learning.
- Parent/carer consent is not required for general supervised used of digital devices as part of the educational program, but written consent is required for the creation and used of children's images, video or audio for purposes outside learning.

- All use of ICT by children is guided by educators, with a focus on educational outcomes and digital literacy.
- Content must be age appropriate, culturally respectful and advertising free.
- Access to the internet is restricted through secure networks and content filtering systems to prevent exposure to harmful or inappropriate material.

Privacy and Data Protection

- All digital records, images, and information about children and families are stored securely in compliance with the Privacy and Data Protection Act 2014 (Vic).
- Parental consent is obtained before collecting, using, or sharing digital content involving children (e.g. photos, videos, or online portfolios).
- Only authorised personnel have access to sensitive or personal digital data.

Child Safety and Empowerment

- Children are supported to develop digital awareness and begin to understand concepts such as privacy, safe sharing, and respectful online interactions in age-appropriate ways.
- Conversations about digital safety are embedded in play-based learning when technology is used.

Use of Generative Artificial Intelligence

- Generative artificial intelligence tools must only be used for appropriate and lawful purposes that supports ECMS work.
- No personal, sensitive or identifiable information about children, families or staff may be entered into AI tools.
- Outputs from AI must not be relied upon without human review and verification.
- Staff must comply with privacy and confidentiality obligations when using AI.

Secure Infrastructure and Monitoring

- ICT systems are protected by security measures such as passwords, antivirus software, and network firewalls.
- Systems and devices are monitored regularly for compliance with online safety protocols.
- Any breaches or concerns regarding online safety are documented, reported, and acted upon in accordance with ECMS's incident management and child protection procedures.

Staff Training and Awareness

- Educators and staff receive regular training on online safety, privacy, and appropriate use of digital technologies in early learning settings.
- Staff are educated on recognising and responding to online risks, including cyberbullying, exposure to inappropriate content, and breaches of privacy.

Family Engagement and Education

- Families are provided with information on online safety practices and how they can support safe technology use at home.
- ECMS encourages open communication with families about the digital tools used in the service and any online safety concerns.

Surveillance Devices

- Families must be informed if CCTV or other surveillance is in use.
- Access to footage is restricted to authorised personnel and for safety, security or compliance purposes only.

Incident Reporting

- Allegations or incidents of physical or sexual abuse, including those involving online environments, must be reported to the Nominated Supervisor/Centre Director immediately and escalated as per the Incident and Reportable Conduct Policy.
- If the allegation relates to a Nominated Supervisor or Centre Director, staff must follow the appropriate policies and procedures.

Preventing Online Harm

- Use of ICT systems for behaviours that may cause harm, including grooming, cyberbullying or sharing inappropriate content is strictly prohibited.

Monitoring and Accountability

ECMS may monitor ICT use for compliance, performance, child protection and security purposes. All use must be attributed to an individual. ECMS may suspend or remove access where risk or breaches are identified.

Roles & Responsibilities

CEO	• Holds ultimate accountability for policy implementation and compliance.
CFO	• Support safe ICT and child safe culture. • Ensure policies are enforced and reviewed. • Uphold compliance obligations.
Director of Risk and Compliance	• Monitors compliance to the policy and investigates potential breaches.
IT Function	• Provide secure systems and approved systems and digital platforms. • Monitor system use and respond to risks. • Implement technical controls to support compliance with this policy. • Maintain secure storage and access protocols for all devices, ensuring child safety is prioritised.

	• Regularly review and update procedures to reflect changes in technology, regulations, and service needs.
Area Managers	• Promote awareness of this policy. • Provide training and guidance on online safety, data protection, and secure equipment use. • Model appropriate use. • Respond to breaches and escalate where required.
Centre Directors/ Nominated Supervisors	• Lead policy implementation across the service. • Ensure all staff, educators, students on placement, contractors and visitors understand and follow expectations around the safe and responsible use of digital devices and online platforms. • Monitor and review use of technology and equipment to ensure compliance with relevant legislation, including the Privacy Act and Child Safe Standards. • Support educators in modelling appropriate digital behaviour for children and families. • Ensure age-appropriate digital content is accessed by children, and that usage aligns with educational and wellbeing outcomes. • Report and respond to breaches of the policy, including inappropriate content access, cybersecurity threats, or misuse of equipment. • Collaborate with families to promote online safety practices at home and in the service.
Educators, Volunteers, Students on Placement, and Contractors	• Use ICT systems lawfully and respectfully. • protect information and privacy especially for children in ECMs services. • report incidents or misuse, security concerns • Follow all ECMS policies and relevant legislation
Parents/Guardians/ Authorised Persons	• Support the service's policy to safe and responsible use of technology and online platforms. • Model respectful and appropriate use of digital devices when on the premises. • Refrain from taking photos, videos, or recordings of children (other than their own) while at the service, unless authorised. • Ensure any personal information or images shared with the service (e.g. via apps or digital communication) respects the privacy of others.

	• Raise any concerns about online safety or equipment use with the Centre Director/Nominated Supervisor promptly. • Respect service policies regarding the use of personal devices (e.g. mobile phones) while on-site. • Keep personal login details for service platforms confidential and notify the service if access is compromised.

Related Legislation, Regulations and Resources

- Education and Care Services National Regulations 2011 (Regs 99-102)
- Privacy Act 1988 (Cth)
- Occupational Health and Safety Act 2004 (Vic)
- National Quality Framework – Quality Area 7
- Child Safe Standards – Standard 9
- National Model Code for Early Childhood Education and Care

Related Policies and Procedures

- Child Safety and Wellbeing Policy
- Code of Conduct
- Complaints and Feedback Policy
- Incident and Reportable Conduct Policy
- Information Security (Cybersecurity) Policy
- Participation of Students and Volunteers Policy
- Privacy and Confidential Information Policy
- Supervision of Children Policy

Document Version History			
Version	**Reason for Amendment**	**Approved by**	**Approval date**
1.0	New policy drafted	ECMS Executive	August 2025