Safe use of digital technologies and online environments policy

PURPOSE

This policy will provide guidelines to ensure that all users of digital technologies at Merri-bek Early Years Management (MEYM):

- understand and follow procedures to ensure the safe and appropriate use of digital technologies, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with the service's *Privacy and Confidentiality Policy*
- promote a child safe culture when it comes to taking, use, storage and destruction images or videos of children
- are aware that only those persons authorised by the Approved Provider are permitted to access digital devices at the service
- understand what constitutes illegal and inappropriate use of digital devices and avoid such activities.
- understand and follow professional use of interactive digital technologies platforms, such as social media *(refer to Definitions)* and other information sharing platforms *(refer to Definitions).*

POLICY STATEMENT

MEYM services are committed to:

- providing a safe environment through the creation and maintenance of a child safe culture, and this extends to the safe use of digital technologies and online environments
- professional, ethical and responsible use of digital technologies at the service
- providing a safe workplace for management, educators, staff and others using the service's digital technologies and information sharing platforms
- the rights of all children to feel safe, and be safe at all times
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of the service's digital technologies complies with all service policies and relevant government legislation
- providing management, educators and staff with online information, resources and communication tools to support the effective operation of the service.

BACKGROUND AND LEGISLATION

The digital technology landscape is rapidly evolving, and early childhood services are increasingly integrating fixed, wireless, and mobile devices to enhance research, communication, and service management. While these tools offer cost-effective and efficient solutions, they also introduce significant legal and ethical responsibilities—particularly around information privacy, cybersecurity, and the protection of children, families, and staff.

Approved Providers and educators must stay informed about emerging technologies and actively manage associated risks, including exposure to harmful content, cyberbullying, and threats amplified by Artificial Intelligence (AI). For instance, digital toys linked to mobile apps can pose cybersecurity risks by allowing unauthorised access to Wi-Fi networks, tracking device locations, and activating audio or video functions—potentially compromising children's safety.

A broad framework of state and federal legislation governs the use of digital technologies in early childhood settings. This includes laws related to privacy, copyright, occupational health and safety, anti-discrimination, and sexual harassment. Unlawful or inappropriate use—such as accessing pornography, committing fraud, defamation, copyright infringement, or engaging in harassment and privacy breaches—can have serious legal consequences. Continuous improvement in online safety practices is essential to protect all members of the service community.

In Victoria, the Regulatory Authority mandates compliance with the National Model Code, a critical guideline for Early Childhood Education and Care (ECEC) services. The Code stipulates that only service-issued devices should be used for capturing photos or videos of children, reducing the risk of unauthorised image distribution. It also requires clear policies for carrying personal devices, ensuring any exceptions are well-justified and tightly controlled. Robust procedures for storing and retaining recordings are vital to safeguarding children's privacy and preventing misuse of sensitive data. Adherence to these standards not only protects children but also builds trust and transparency between services and families.

A wide range of legislation and standards govern practices across media, education, privacy, safety, and human rights in Australia. Key federal and Victorian laws include the *Broadcasting Services Act 1992*, *Copyright Act 1968*, *Privacy Act 1988*, *Crimes Act 1958 (Vic)*, and *Equal Opportunity Act 2010 (Vic)*. These are complemented by regulations such as the *Education and Care Services National Law Act 2010*, the *National Quality Standard – Quality Area 7*, and the *Occupational Health and Safety Act 2004 (Vic)*. Together, they ensure compliance, protect individual rights, promote transparency, and uphold governance standards across sectors.

SCOPE

This policy applies to all Approved Providers, nominated supervisors, persons in day-to-day charge, early childhood teachers, educators, staff, students, and volunteers engaged with Merri-bek Early Years Management (MEYM). It does not apply to children. While digital technologies may be used within educational programs, guidance on their safe use with children is outlined in the MEYM eSafety Policy.

The scope of this policy encompasses all aspects of digital technology use, including but not limited to:

- Desktop computers, laptops/notebooks, tablets, iPads, smartphones, and smart devices
- Copying, saving, or distributing files
- Email communication
- File sharing and storage (including endpoint data storage devices)
- Cloud-based file transfer and storage
- Instant messaging platforms
- Internet usage
- Portable communication devices, including mobile and cordless phones
- Printing and distribution of materials
- Social media usage (see Definitions)
- Streaming media services
- Subscriptions to list servers, mailing lists, or similar services
- Video conferencing tools
- Blogs and vlogs

This policy ensures responsible, secure, and ethical use of digital technologies across all MEYM services and roles.

Responsibilities of the **Approved Provider and Persons with Management or Control** include:

- Ensuring compliance with legislation, regulations, and service policies on digital technologies, privacy, and confidentiality
- Overseeing risk assessments, policies, and procedures to minimise risks to children’s health, safety, and wellbeing
- Maintaining oversight of image, video, and data storage, access, and transfer to protect children’s privacy
- Providing secure systems, devices, and facilities for staff use, including password protection and backups
- Providing sufficient service-issued devices for staff to use, including during excursions and off-site programs
- Ensuring staff only use organisational devices to prevent staff from transferring children’s images to personal accounts, devices, or social media platforms
- Authorising access to digital technologies and ensuring appropriate training for staff
- Embedding a culture of child safety, wellbeing, and responsible digital use across the service

Responsibilities of the **Nominated Supervisor and Persons in Day-to-Day Charge** include:

- Implementing policies and procedures in daily practice, including supervision of children using digital technologies
- Conducting and documenting risk assessments for the use service-issued devices
- Ensuring staff follow privacy requirements when capturing, storing, or sharing images and recordings
- Monitoring staff use of service-issued devices to ensure appropriate and lawful use Supporting staff to comply with safe use of personal devices, including restrictions within the classroom and service
- Managing inappropriate use of digital technologies and responding to breaches promptly
- Ensuring sufficient numbers of service-issued devices are available for staff
- Supporting staff to restrict children's access to technology to short, purposeful, and developmentally appropriate activities

Responsibilities **of Early Childhood Teachers, Educators and all other staff** include:

- Actively supervising children when using digital technologies ensuring use is limited, purposeful, and age-appropriate
- Following service policies on privacy, confidentiality, and safe device use
- Asking children for permission before taking photos or videos and explaining their use
- Using only service-issued devices for work purposes and keeping personal devices stored securely during sessions
- Not using personal devices within the classroom and playground spaces
- Reporting hazards, inappropriate use, or breaches to supervisors promptly
- Maintaining security of passwords, files, and devices, and ensuring fair access to digital resources
- Ensuring that images and recordings of children are stored securely and never transferred to personal devices

Families play a vital role in supporting the service's health and safety goals. Their responsibilities include:

- Providing consent for images, videos, and digital access where required
- Respecting service policies by not taking photos or recording children on personal devices during events or within the service
- Not using personal devices within the classroom and playground spaces
- Communicating openly with staff about digital safety concerns or privacy issues
- Supporting children's safe and responsible use of digital technologies at home
- Collaborating with educators to promote consistent safety and wellbeing practices

Contractors, volunteers and students are required to comply with all aspects of MEYM's policies.

DEFINITIONS

A glossary of definitions can be found on our website.

PROCEDURES

The Approved Provider, nominated supervisors, persons in day-to-day charge, early childhood teachers, educators, staff, students, and volunteers engaged with Merri-bek Early Years Management (MEYM) are required to acknowledge their understanding of and commitment to this policy and to the procedures outlined herein at all times. Compliance with these procedures is essential to ensure the safe, ethical, and lawful use of digital technologies across all MEYM services.

POLICY REVIEW

To ensure the values and objectives of this policy are effectively met, the Approved Provider will implement a continuous evaluation process. This includes regularly seeking feedback from all stakeholders impacted by the policy, monitoring its

implementation, compliance, and any related complaints or incidents. The policy will be kept current with relevant legislation, research, and best practice, and revised as part of the service's scheduled review cycle or when necessary. In accordance with Regulation 172(2), all affected stakeholders will be notified at least 14 days prior to any significant changes to the policy or its procedures, unless a shorter timeframe is required due to potential risk.

Approving Authority	**General Manager**
Date Approved	August 29th 2025
Date Effective	September 1st 2025
Policy Owner	MEYM
Policy Category	Mandatory Policy
Edition	V1
Review Date	January 2026

This policy and its contents were referenced from Early Learning Association Australia (ELAA).

Procedure 1: Use of Digital Technologies at MEYM

Email use

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- MEYM employees should use the MEYM email signature block that identifies employee name, title, service name, service phone number and address
- MEYM staff should include the MEYM disclaimer which is common to all users, on emails to limit liability.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself. If you receive an unusual file or program, please contact MEYMs IT support or GM for advice.
- Never open emails if unsure of the sender.
- All correspondence with families should be sent to and from the service email account. Staff should not use their personal MEYM email address for correspondence with external parties.
- Remove correspondence that is no longer required from the computer quarterly.
- MEYM staff should use an 'out of office' auto reply to advise families of their working days and an expected turnaround time or alternative contact for extended periods of leave and on all service email addresses
- Never send unauthorised marketing content or solicitation emails
- Be suspicious of phishing titles.

Digital storage of personal and health information

Digital records containing personal, sensitive and/or health information, or images of children must be password protected and stored securely so that privacy and confidentiality is maintained. This information must not be removed from the service without authorisation, as security of the information could be at risk

Digital records containing personal, sensitive and/or health information, or images of children may need to be removed from the service from time-to-time for various reasons, including for:

- excursions and service events (refer to Excursions and Service Events Policy)
- offsite storage, to retain records for long term storage

In such circumstances, services must ensure that the information is transported, handled and stored securely so that privacy and confidentiality is maintained at all times.

- Images, recordings, and other information relating to children that are no longer required or in active use must be deleted from service devices at the end of each week to ensure privacy and data security
- Personal storage devices must not be used to transfer MEYM data or information between MEYM devices, to ensure data security and prevent unauthorised access.
- Digital technology users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.
- Ensure all material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secure location.
- Personal devices must not be used within the service for any purpose—whether personal or work-related—including the sharing of information, images, recordings, or personal details of children

Backing up data

Data backup is the process of creating accessible data copies for use in the event of breach or loss. MEYM partners with Cornerstone IT to ensure a safe backup of files are stored in a cloud-based server. MEYM staff should save files to the Box drives installed on each computer or in Google drives instead of on your local desktop to ensure that files are secure and can be retrieved in the event of a local system error.

Password management

The effective management of passwords is the first line of defence in the electronic security of an organisation. All MEYM devices should be protected by passwords or other security mechanisms to prevent unauthorised access of files and data. MEYM staff should not use a password or login details for any other person to gain access to MEYM platforms, files, emails or data.

A strong password should:

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#$%^&*()_-+=)
- always verify a user's identity before resetting a password
- change passwords when an employer leaves the service
- password rotation; changed every 90 days or less
- do not use automatic logon functionality
- use of account lockouts for incorrect passwords, with a limit of 5 or fewer bad attempts.

Users should always follow these principles:

- do not share passwords with anyone.
- never use the same password for work accounts as the one you have for personal use (banking, etc.).
- do not write down passwords or include them in an email.
- do not store passwords electronically unless they are encrypted.
- never use the "remember password" feature on any systems; this option should be disabled
- Do not use the same password for multiple administrator accounts.

Working from home

When an Approved Provider, nominated supervisor, early childhood teachers, educators or staff members are working from home they must:

- Obtain prior approval for each instance of remote work
- complete the authorised user agreement form
- conduct a workstation assessment; taking reasonable care in choosing a suitable work space, including ergonomics, lighting, thermal comfort, safety, and privacy
- ensure security and confidentiality of work space, keeping private, sensitive, heath information, planning, educational programs and children's records confidential and secure at all times
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- adhere to the Privacy and Confidently Policy
- report breaches to privacy or loss of private, sensitive, and heath information to the General Manager as soon as practically possible.
- Ensure that no device is taken outside of the service environment that contains images or recordings of children

Procedure 2: Unacceptable or Inappropriate Use of Digital Technology

Users of the digital technologies facilities (and in particular, the internet, email and social media) provided by MEYM must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails spam or other unauthorised mass communication
- use the digital technology facilities as a platform to gain unauthorised access to other systems
- carry out activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation
- use the digital technology facilities to access, download, create, store or distribute illegal, offensive, obscene or objectionable material (including pornography and sexually explicit material). It will not be a defence to claim that the recipient was a consenting adult
- use the digital technology facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of [Company]
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- use the facilities to assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by [Company] unless authorised as part of their duties
- publish the service's email address on a 'private' ebusiness card
- harass, slander, intimidate, embarrass, defame, vilify, seek to offend or make threats against another person or group of people
- breach copyright laws through making copies of, or transmitting, material or commercial software.

Breaches of this policy

Use of the service's digital technology facilities must comply with all legal and policy requirements. Individuals who engage in unlawful activities using these technologies may face serious consequences, including criminal or civil legal action, fines, damages, or imprisonment. The Approved Provider will not defend or support any individual found to be using the service's digital systems for unlawful purposes. Where inappropriate use is identified, the organisation reserves the right to block access to internet sites. Failure to adhere to this policy may result in counselling, disciplinary action, dismissal, or restricted access to digital technology facilities for management, educators, staff, volunteers, and students.

Category 1: illegal — criminal use of material

This category includes but is not limited to:

- child abuse material offences relating to child pornography covered by the Crimes Act 1958 (Vic). 'Child abuse material' is defined in section 51A of the Crimes Act 1958 (Vic)
- objectionable material — offences relating to the exhibition, sale and other illegal acts relating to 'objectionable films' and 'objectionable publications' covered by the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic). Such material has or would attract a classification of X18+ (restricted) or RC (refused classification) under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth)
- reckless or deliberate copyright infringement and any other material or activity that involves or is in furtherance of a breach of criminal law

Category 2: extreme — non-criminal use of material

This category includes non-criminal use of material that has or may attract a classification of RC or X18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth).

This includes any material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult or a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not)
- promotes, incites or instructs in matters of crime or violence
- includes sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults

Category 3: critical — offensive material

This category includes other types of restricted or offensive material, covering any material that:

- has or may attract a classification of R18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). Material may contain sex scenes and drug use that are high in impact
- includes sexualised nudity
- involves racial or religious vilification
- is unlawfully discriminatory
- is defamatory
- involves sexual harassment or bullying

Category 4: serious

This category includes any use which is offensive or otherwise improper.

The categories do not cover all possible breaches of this policy. Matters not covered by the above categories will be dealt with on an individual basis and on the relevant facts.

Procedure 3: Social Media and Information Sharing Platform Guidelines

The below directives are essential to the safety and wellbeing of staff, children and their families, and to ensure that Merri-bek Early Years Management (MEYM) operates in a professional and appropriate manner when using social media and/or information sharing platforms.

Staff must exercise extreme caution using digital technology devices when accessing social media and/or information sharing platforms, whether in the workplace or relating to external events or functions involving MEYM.

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff or management from MEYM on social media sites without the express consent or authorisation of the General Manager. It is also an offence under current legislation, to record or use a visual image of a child, including transmitting the image on the internet, without the written consent of the child's parent.

MEYM specifically requires that, unless you have the express permission, you:

- Do not video or photograph anyone, or post photos or personal details of other MEYM staff, children or families;
- Do not post photos or videos of staff, children or families on your personal Facebook page, or otherwise share photos or videos of staff, children or families through social media;
- Do not create a MEYM branded Facebook page, or other pages or content on social media that represents MEYM, it's staff, children or families;
- Do not post anything that could embarrass or damage the reputation of MEYM, colleagues, children or families.

Staff must not:

- post or respond to material that is, or might be construed as offensive, obscene, fraudulent, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful or inaccurate;
- make any comment or post any material that might otherwise cause damage to MEYM's reputation or bring it into disrepute;
- imply that they are authorised to speak as a representative of MEYM, or give the impression that the views expressed are those of MEYM unless authorised to do so
- use a MEYM email address or any organisational logos or insignia that may give the impression of official support or endorsement of personal comments;
- use the identity or likeness of another employee, contractor or other member of MEYM
- use or disclose any confidential information or personal information obtained in the capacity as an employee/contractor of MEYM or
- access and/or post on personal social media during paid workhours.

Personal use of social media

MEYM recognises that staff may choose to use social media in their personal capacity. This policy is not intended to discourage nor unduly limit staff using social media for personal expression or other online activities in their personal life. Staff should be aware of and understand the potential risks and damage to MEYM that can occur through their use of social media, even if their activity takes place outside working hours or on devices not owned by MEYM.

If an individual can be identified as an employee of Merri-bek Early Years Management on social media, that employee must:

- only disclose and discuss publicly available information;
- ensure that all content published is accurate and not misleading and, complies with all relevant policies of MEYM
- expressly state on all postings (identifying them as an employee of MEYM) the stated views are their own and are not those of MEYM;
- be polite and respectful to all people they interact with;
- adhere to the Terms of Use of the relevant social media platform/website, as well as copyright,
- abide by privacy, defamation, contempt of Court, discrimination, harassment and other applicable laws;

- ensure that abusive, harassing, threatening or defaming postings which are in breach of MEYM policies may result in disciplinary action being taken, even if such comments are made using private social networks outside of working hours.
- notify the General Manager or Area Manager if they become aware of unacceptable use of social media as described above.

Consequences of unacceptable use of social media

- MEYM will review any alleged breach of this policy on an individual basis. If the alleged breach is of a serious nature, the person shall be given an opportunity to be heard in relation to the alleged breach.
- If the alleged breach is clearly established, the breach may be treated as grounds for dismissal. In all other cases, the person may be subject to disciplinary action in accordance with MEYM's *Code of Conduct Policy*.
- MEYM may request that any information contained on any social media platform that is in breach of this policy be deleted.
- MEYM may restrict an employee's access to digital technology facilities or if they are found to have breached this policy or while MEYM investigates whether they have breached this policy.