

Safe Use of Digital Technology and Online Environments Policy



1. Purpose

Children's safety and wellbeing are paramount in our services. This includes ensuring the safe use of digital technologies and online environments to support children's learning and development and maintaining records.

The purpose of this policy is to provide clear guidelines for the safe use of digital technology and online environments for staff, children, and young people and to monitor and limit the use of electronic devices and use of children's images in MACSEYE services to ensure child-safe practices.

MACSEYE is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and community. As a child safe organisation, MACSEYE embeds Victorian Child Safe Standards and continuously addresses risks to ensure children are safe in physical and online environments. Digital technologies have become an integral part of many children's daily lives. For this reason, it is important that our educators are not only familiar with the use of digital technologies, but are able to guide children's understanding of, and ability to interact, engage, access and use a range of digital technology in a child safe environment.

2. Scope

This policy applies to children, families, staff, management, volunteers and visitors (including contractors) of any MACSEYE Service.

3. Background

The *Education and Care Services National Regulations* require approved providers to ensure their services have policies and procedures in place for the safe use of digital technologies and online environments at the service.

Establishing child safe practices for the use of electronic devices and online environments is essential to safeguarding children from harm and abuse and prioritising their safety and wellbeing.

Our services use digital technology and electronic devices as a tool for learning with children, documenting their learning and development, communicating with families and the wider community, supporting program planning and administration tasks and enhancing safety and security through systems such as sign in/out platforms and CCTV monitoring. In the event children are using their own device at the service, our educators are diligent in supervision practice to prevent children accessing inappropriate material.

The National Model Code

The National Model Code has been developed to support approved providers to create a child safe culture when it comes to taking, sharing and storing images or videos of children at their services.

MACSEYE adheres to the National Model Code under the National Quality Framework to ensure MACSEYE services promote a child-safe culture. The National Model Code guides the electronic practices of approved providers, staff, families, and volunteers while children are present at the centre.

4. Policy

DEVICE MANAGEMENT

Personal electronic devices

MACSEYE service staff are not permitted to carry personal electronic devices or personal storage media devices while children are at the service. Staff must store personal electronic devices or personal storage media devices away in a secure location such as their bag in the staff office, at the beginning of each shift. MACSEYE staff are permitted to access their personal electronic devices during their breaks without children present (for example, when in the staff room or outside the service).

MACSEYE informs staff, educators, visitors, volunteers and family members that the use of personal electronic devices used to take photos, record audio or capture video of children who are being educated and cared for at the Service is strictly prohibited. This includes items such as tablets, phones, digital cameras, smart watches capable of taking images, META sunglasses and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage). These devices should not be in the possession of staff, educators or visitors (e.g. inclusion support or allied health professionals) while working directly with children.

Essential identity photographs

MACSEYE may collect a photograph of children upon enrolment for medical management and identification purposes, for example a photo must be included on a child's medical action plan to ensure educators can easily identify children with medical conditions to effectively manage the condition.

MACSEYE-issued electronic devices

Each MACSEYE service is provided authorised electronic devices (such as a phone, laptops and iPads). These are used to record attendance, access child information and perform routine checks (such as headcounts and monitoring the UV rating) and to capture images for the educational program. The use of MACSEYE-issued devices by staff should adhere to the Technologies Acceptable Use Policy.

All devices must be secured at the end of each day and remain at the premises. Staff and educators are advised that electronic devices belonging to the service must not be removed from the premises as they may contain personal details of staff or children, including photos or videos. Except where required for operational activities, for example excursions or transportation.

Essential phone use

MACSEYE service staff (educators) should inform families and/or emergency contacts, and their children's schools or childcare providers, of the service contact details to ensure they are contactable in personal emergencies.

Under certain circumstances, staff, educators and visitors may require an exemption to use or be in possession of a personal electronic device that can be used to take images or videos. The employee must obtain a written exemption from the General Manager – Services, to carry their personal device while children are present. Instances that may be authorised include:

- a personal health requirement – for example, for blood sugar monitoring
- disability – for example, if a personal electronic device is used as an essential means of communication
- family necessity – for example, having a family member with a serious illness
- a local emergency or technical outage – for example, anticipating a bushfire evacuation text notification.

In cases of exemption, and with the employee's consent, the Area Manager should notify other staff about arrangements for the employee's personal electronic device. The reason for the exemption does not need to be

shared. Service staff with an exemption to carry their device must not use their personal device to take images or videos of children.

Staff are permitted to use their personal electronic devices during an emergency to communicate with emergency services. This includes situations involving a lost child, an injured staff member or child, or a lockdown or evacuation (see the Emergency and evacuation policy and procedure). In the event this has occurred, they are required to notify their Area Manager.

Excursions

Staff are required to bring at least one MACSEYE-issued mobile phone on excursions to ensure they can be contacted (see the *Excursions and Incursion policy and procedure*).

USE OF IMAGES

This policy identifies who is authorised to take, use, store and destroy images and videos of children using a MACSEYE issued digital devices. Images and videos will be stored securely in MACSEYE approved applications and systems only, with access limited to authorised personnel only.

Images and videos of children must only be taken and used in accordance with MACSEYE policies, and careful consideration given to the purpose of the image or video. Requirements for the use and storage of children's images includes:

- Educators are to consider the intent, appropriateness, context and consent involved in capturing and using the images and videos, ensuring the process aligns with children's learning, wellbeing and right to privacy.
- Coordinators and Centre Directors must ensure they have obtained parent authorisation and child consent (as per the table below), prior to taking any images.

Images or videos of children may be taken on service iPads and stored on the following MACSEYE platforms for the purpose of documentation relating to children's learning, enrolment, medical management and incident management:

- Childcare Management System, Incident Management Platform, Family Communication Platform.

Images or videos of children must not be stored or shared on:

- Emails, Microsoft Teams Platform, SharePoint, OneDrive and/or File Explorer, other than, for the approved purpose of QIPs and Medical Management.

MACSEYE services will regularly review how digital data, including images and videos of children, is stored, including back-ups of all digital data, whether offline or online (such as a cloud-based services). Digital data stored at the service will be destroyed when no longer required. MACSEYE will take measures to prevent any staff, educator, visitor and volunteer transferring images or videos from a MACSEYE issued device to personal devices. Unauthorised transferring of digital data may result in disciplinary action and/or report to relevant authorities.

Educational program and practice

MACSEYE believes that safe technology use has a place in children's learning. Technology can make learning more interactive and engaging for children and support in the process of interest-based learning by providing powerful research tools. Moreover, images and videos can be used by educators to capture evidence of learning that may be shared with families and allow children to re-visit their learning.

Where appropriate, physical photographs of children may feature in the educational program, Quality Improvement Plan (QIP) and service environment.

All images and videos of children are deleted annually, at the end of the year.

Authorisations and Consent

In line with our educational philosophy and commitment to ensuring children's voice is captured as part of the educational program, educators will ask children's permission prior to taking their photo or video and respect the child's wishes.

Authorisation from parents or authorised nominees to take, use and store images and videos of children being educated and cared for by the service are captured in a multilayered approach, as detailed below:

STAGE	CONSENT	WHO
Enrolment	Images of children taken with service issued devices for the purpose of documenting children's learning: - family communication application - educational program - service newsletters - displayed in the educational environment	Parents or authorised nominees
Enrolment	Images of children taken with service issued devices for the purpose of: - children's medical management - identifying children on the service allergy buddy	Parents or authorised nominees
Enrolment	Images of children taken with service issued devices in the enrolment Childcare CRM platform for the purpose of identification of enrolled children	Parents or authorised nominees
In service	Images of children taken with service issued devices used for: - external marketing - internal staff training	Parents or authorised nominees
In service	Children's use of digital devices while in the service	Parents or authorised nominees

Public use of images

MACSEYE may engage a professional photographer to capture images or videos featuring children at the centre.

These images will be captured in a way that does not identify individual children. This may include photographs taken from behind, at a distance, from above, or focused on non-identifying features such as hands or feet, so that faces and other identifying characteristics are not visible.

These images may also be used on MACSEYE public platforms, including social media, websites, marketing brochures and email communications. Families will be informed in advance, and a parent or carer will need to provide written consent for their child's image to be included and published, as per the authorisations above. Occasionally, a professional photographer may be engaged include:

- for special events – for example, centre-based special events
- for public content – for example, to use in social media, on the MACSEYE website or on the Department of Education website.

MACSEYE may receive requests from other government departments, agencies or ministers to provide images featuring children at the centre or wish to use images that include children in promotional materials. MACSEYE

will inform families in advance, and a parent or carer will need to provide written consent for their child's image to be included and published.

MACSEYE will take reasonable steps to protect children's privacy by ensuring any images used for the above purposes are captured in a way that does not identify individual children.

Special events

Area Managers are responsible for determining whether photographs or videos can be appropriately captured at special events. They are also responsible for informing parents in advance if there will be images captured and where those images will be used.

Area Managers will consider the context of the event and communicate this decision in advance to families. No images or videos captured by families at a special event are permitted to be published on social media, websites or other online platforms.

ONLINE SAFETY

Physical Environment and Active Supervision

Where it has been assessed as appropriate for children to engage in the use of devices, Service staff, including Coordinators, Centre Directors and Educators will:

- ensure children are always supervised and never left unattended whilst an electronic device is connected to the internet
- provide a child safe environment to children- reminding them if they encounter anything unexpected that makes them feel uncomfortable, scared or upset, they can seek support from staff
- reflect on our Service's physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology
 - perform regular audits to identify risks to children's safety and changes in room set-ups that can indicate areas of higher-risk and become supervision 'blind spots'
 - ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members when working with children
 - only permit children to use devices in open areas where educators can monitor children's use
 - be aware of high-risk behaviours for children online, including uploading private information or images, engaging with inappropriate content (inadvertently or purposefully), making in-app purchases, and interacting with unsafe individuals
 - ensure all visitors and volunteers are supervised at all times
 - ensure all devices are password protected with access for staff only, except in the event of being used for the purpose to sign in and out.
- where digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure.

Software programs and apps

MACSEYE uses a range of secure software programs and apps on Service-issued devices to support the educational program and administration of our services. All apps used by staff and educators, are carefully selected, regularly checked and kept up to date with the latest available system updates. Access to software programs and apps are password protected to ensure the privacy of children, families and staff. Each user has their own user account, and they need to ensure log in, and password information is not shared. In the event of a shared account or guest user access (to ensure casual or relief educators can access information required for service provision), MACSEYE will implement necessary controls to secure the accounts and sensitive data.

MACSEYE will ensure programs which require additional background checks, such as CCS Software, are only accessed by authorised staff who have completed necessary screening processes in accordance with Family Assistance Law. Our educational program software is used by educators to share observations, photos, videos, daily reports, and learning portfolios with families in a secure, closed platform. In addition, our central support office may use accounting and payroll software such as MYOB or Xero, HR systems, and compliance tools. These platforms assist in managing the Service's financial, staffing, and operational requirements.

Artificial Intelligence (AI)

Educators or staff using AI are to be aware of limitations, privacy risks, and the potential for errors in the information it provides. AI can support and assist staff as a documentation tool; however, it is their responsibility to ensure the information's accuracy and not rely upon it as an authoritative source. Educators and other service staff are required to consult with their Area Manager prior to using AI tools regarding the purpose and intended practice, to ensure these tools are applied safely. Staff and educators should ensure they enter original work into the AI program and are required to monitor, verify, and check information obtained from AI to ensure specific details are contextually relevant.

Data and privacy concerns must be addressed, and staff should not enter any MACSEYE information, particularly personal or sensitive data e.g. child names and date of birth, into publicly available generative AI tools. Only MACSEYE approved AI programs may be used with your MACSEYE email address/ user account and MACSEYE classified information.

Use of Closed-Circuit Television (CCTV)

The use of CCTV systems may be deemed appropriate to ensure the health, safety and wellbeing of children, staff, families and visitors to a service. The use of CCTV supports MACSEYE services to act as a deterrent to misconduct and inappropriate behaviour and reduce the likelihood of crime. It supports the management and investigation of emergencies, incidents or allegations and helps to verify incidents on premises to support an evidence-based response.

In services where CCTV systems are in place, the following parameters and conditions apply:

- any third party engaged to install CCTV systems are qualified and licensed and systems are maintained and serviced as per manufacturer instructions
- clear signage will be in place to inform staff, children and families that CCTV may capture their image in line with the Privacy Act 1988
- images or personal information captured on CCTV is stored securely and destroyed or de-identified when it is no longer needed in line with the Privacy Act 1988
- CCTV cameras will be clearly visible and not concealed in any way
- CCTV systems are not in places where people expect privacy, such as bathrooms or nappy change areas
- CCTV images are only accessible to authorised persons (see definition of 'authorised person') in certain circumstances (outlined below) and are destroyed within specified timeframes

Only authorised persons may view footage and images recorded by CCTV systems in certain circumstances, including:

- for the purpose of internal or external investigation or review of an emergency, incident or allegation
- for the purpose of identifying misconduct or inappropriate behaviour

REPORTING OF SAFETY CONCERNS

MACSEYE Services will implement measures to keep children safe whilst using digital technology and accessing online environments. All staff receive training and induction on their obligations to report concerning conduct, breach of MACSEYE policy and/or any circumstance which may pose a risk to children. All educators are required to acknowledge their understanding and adherence to the National Model Code.

The Area Manager will:

- ensure all staff, educators, students and volunteers are aware of their mandatory reporting obligations and promptly report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor in line with the Child Safety and Wellbeing Policy.
- support educators to:
 - encourage children to seek support if they encounter anything unexpected that makes them feel uncomfortable, scared or upset
 - listen sensitively and respond appropriately to any disclosures children may make relating to unsafe online interactions or exposure to inappropriate content
 - respond to and report any data breaches or incidents of inappropriate use of digital devices and online services to management
- ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required
- report any suspected cases of online abuse to the relevant authorities, including the eSafety Commissioner and Police, in accordance with legal requirements and child protection procedures
- notify the regulatory authority within 24 hours, via NQAITs, if a child is involved in a serious incident, including any unsafe online interactions, exposure to inappropriate content, or suspected online abuse.

CONFIDENTIAL AND PRIVACY GUIDELINES

Our Privacy Policy applies to all use of digital technology and online environments. All staff, educators, contractors and visitors must ensure that any information, images and digital content relating to children, families, employees and the Service are collected, accessed, stored, used, and shared only in accordance with privacy legislation, MACSEYE policies and approved procedures.

Any actual, suspected or potential privacy breach, information security incident, cyber security event, loss of equipment, unauthorised disclosure of personal information or unauthorised access to Service information must be reported immediately to the Area Manager and Safety and Compliance Team. Staff must not attempt to conceal, delete or independently manage the incident.

The Safety and Compliance Team will assess reported incidents and, where required, escalate them to the Privacy Officer and activate the Data Breach Response Process, including notification under the Notifiable Data Breaches Scheme and reporting to the Office of the Australian Information Commissioner (OAIC).

Examples of incidents requiring immediate reporting include:

- loss or theft of a device containing personal information;
- unauthorised access to a database or system containing personal information;
- sending personal information, reports, photographs or documentation to the wrong recipient;
- disclosure of confidential information through email, messaging applications, cloud platforms or unapproved AI tools;
- phishing, malware or ransomware incidents;
- any privacy or information security incident occurring at the Service or while undertaking excursions, transport or other off-site activities.

Staff must also comply with their child safety and mandatory reporting obligations. Any concerns regarding inappropriate use of digital technology affecting the safety or wellbeing of a child must be reported immediately in accordance with MACSEYE's Child Safety and Mandatory Reporting procedures.

5. Induction and ongoing training

This policy will be accessible by service staff via the info hub (intranet) and by families via the website. A hard copy of the policy will be available through the Service. Area Managers are responsible for ensuring staff access to the policy and any supporting documents and undertake induction training prior to the policy being implemented. All service staff are responsible for understanding and complying with this policy and ongoing training will be provided using a range of learning platforms.

6. Related documents

- Code of Conduct Policy
- Enrolment and Orientation Policy
- Privacy Policy
- Participation of Volunteers and Students
- Technologies Acceptable Use Policy
- Staffing Arrangements Policy
- Child Safety and Wellbeing Policy
- Code of Conduct Policy
- Responsible Person Policy
- Medical Conditions Policy

7. Legislative requirements

NATIONAL QUALITY STANDARDS (NQS)	
Quality Area 2	Children's Health and Safety
Quality Area 7	Governance and Leadership

EDUCATION AND CARE SERVICES NATIONAL LAW 2010	
Section 162A	Child protection training
Section 165	Offence to inadequately supervise children
Section 167	Offence relating to protection of children from harm and hazards

EDUCATION AND CARE SERVICES NATIONAL LAW REGULATIONS 2011	
Regulation 84	Awareness of child protection law
Regulation 115	Premises designed to facilitate supervision

Regulation 168	Education and care services must have policies and procedures
Regulation 168(ha)	The safe use of technologies and online environment at the service
Regulation 122	Educators must be working directly with children to be included in ratios
Regulation 123	Educator to child ratios – centre-based services
Regulation 170	Policies and Procedures to be followed
Regulation 171	Policies and Procedures to be kept available
Regulation 172	Notification to change to Policies or Procedures
Regulation 181	Confidentiality of records kept by approved provider
Regulation 195	Application of Commonwealth Privacy Act 1988
Regulation 196	Modifications relating to National Education and Care Services Privacy Commissioner and Staff

RELATED LEGISLATIONS
A New Tax System (Family Assistance) Act 1999 (Cth)
Family Law Act 1975 (Cth)
Information Privacy Act 2000 (Vic)
Occupational Health and Safety Act 2004 (Vic)
Privacy Act 1988 (Cth)

8. Definitions

Term	Meaning
Adequate supervision	Means: - An educator can respond immediately, particularly when a child is distressed or in a hazardous situation - Knowing where children are at all times, and monitoring their activities actively and diligently
Approved first aid qualifications	A qualification that includes training in the matters set out below, that relates to and is appropriate to children and has been approved by ACECQA and published on the list of ACECQA's approved first aid qualifications and training. Matters are likely to include emergency life support and cardiopulmonary resuscitation; convulsions; poisoning; respiratory difficulties; management of severe bleeding; injury and basic wound care; and administration of an auto-immune adrenalin device.

Approved provider	A person who holds a provider approval (National Law). A provider approval authorises a person to apply for one or more service approvals and is valid in all jurisdictions.
Artificial intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation
Authorised person	As it relates to the use of CCTV, an authorised person is the • Nominated Supervisor • Approved provider being a person with management or control or • A person delegated with the authority to view CCTV footage by a person with management or control in certain circumstances (i.e. for investigation or incident review)
Education and care service premises	In relation to a centre-based service, it means each place at which an education and care service operates or is to operate.
Educational program	A program that: • is based on an approved learning framework; and • is delivered in a manner that accords with the approved learning framework; and • is based on the developmental needs, interests and experiences of each child; and • is designed to consider the individual differences of each child (National Law).
Excursion	An outing organised by an education and care service but does not include an outing provided on a school site
MACS	MACS is a reference to Melbourne Archdiocese Catholic Schools Ltd.
MACSEYE	Melbourne Archdiocese Catholic Early Years Education Ltd, a subsidiary of Melbourne Archdiocese Catholic Schools Ltd established to conduct early childhood education and care services.
National Law	Unless otherwise specified, the Education and Care Services National Law Act 2010 or, in Western Australia, the Education and Care Services National Law (WA) Act 2012. This applied law system sets a national standard for children's education and care across Australia. See the ACECQA website for the Application Act or legislation that applies in each jurisdiction.
National Regulations	The Education and Care National Regulations. National Regulations support National Law by providing detail on a range of operational requirements for an education and care service.
Nominated supervisor	In relation to an education and care service, means a person who: • is nominated by the approved provider of the service under Part 3 to be a nominated supervisor of that service; and • unless the individual is the approved provider, has provided written consent to that nomination (National Law).

Person in day-to-day charge	A person is in day-to-day charge of an education and care service if: - the person is placed in day-to-day charge by the approved provider or a nominated supervisor of the service; and - the person consents to the placement in writing (National Regulations). There are minimum requirements for the person in day-to-day charge.
Person with management or control	In relation to education and care services, means: - if the provider or intended provider of the service is a body corporate, an officer of the body corporate within the meaning of the Corporations Act 2001 of the Commonwealth who is responsible for managing the delivery of the education and care service; or - if the provider of the service is an eligible association, each member of the executive committee of the association has the responsibility, alone or with others, for managing the delivery of the education and care service; or - if the provider of the service is a partnership, each partner who has the responsibility, alone or with others, for managing the delivery of the education and care service; or - in any other case, a person who has the responsibility, alone or with others, for managing the delivery of the education and care service (National Law).
Risk assessment	A systematic process of evaluating the potential likelihood and consequences of risks that may be involved in a projected activity or undertaking.

9. Policy information

Policy information			
Policy title:	Safe Use of Digital Technologies and Online Environments Policy	Version:	2.0
Authorised Executive:	Director – Quality, Safety and Compliance	Responsible Manager:	Director – Quality, Safety and Compliance
Approving authority:	Managing Director	Approval date:	25/08/2025
Effective date:	25/08/2025	Review date:	25/08/2026
Review approval date:	16/09/2026	Next review date	16/09/2027

Version control		
Version	Date	Changes
1	25/08/2025	Draft Policy approved
1.1	18/06/2026	Annual review of Policy undertaken, including; • Alignment with the current approved MACSEYE policy template. • Updates to governance, accountability and approval references to reflect current organisational requirements. • Clarification of privacy, information security and data breach management obligations. • Enhanced guidance regarding the collection, use and protection of children's images. • General refinements to policy structure, language and formatting to improve clarity, consistency and usability.
2.0	16/09/2026	Updated Policy approved