Safe use of digital technologies and online environments policy

This is a mandated policy under the operational policy framework. Any edits to this policy must follow the process outlined on the creating, updating and deleting operational policies page.

1. Overview

This policy outlines the department's child safe practices when using digital technologies and online environments in early childhood education and care (ECEC) services and programs. It includes:

- ensuring that no employee, volunteer or contractor can use personal electronic devices that can take images or videos (such as mobile phones, digital cameras, tablets, smart watches and other new and emerging technologies, where those technologies have image taking or video recording capability) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage), when working with children.
- the safe use of service issued devices including mobile phones and tablets and any other device that can take images and video.
- requirements for safe taking, use, sharing, storage and destruction of images and videos of children.
- optical surveillance devices such as closed-circuit television (CCTV)
- devices used by children.
- emerging technologies such as Artificial intelligence (AI).

2. Scope

This policy applies to all staff and volunteers working with or providing a service to children and young people in the department's ECEC services and programs, including:

- staff and volunteers working in early education and care sites and programs
- other government staff regularly assigned to a service or program (i.e. DHS Community Development Coordinator)
- work placement students working in early education and care sites and programs
- leaders and employees in corporate office
- employees and volunteers of School Governing Councils with a school-based preschool and Preschool Governing Councils
- employees and volunteers of external and contracted service providers.

For the remainder of this policy, references to 'staff and volunteers' will encompass all the positions listed above.

In scope of this policy is all centre-based department sites, services and programs delivering ECEC services and programs including:

- children's centres
- crèche
- integrated services with long day care programs
- learning together communities
- occasional care
- playcentres
- playgroups
- preschools including school-based preschools
- rural care

This policy also applies when children are transported by, or on, transport arranged by an ECEC service and program.

Visitors at the service, as a condition of entry must agree in writing that they will not take any images or videos of children throughout the visit. All visitors will be directly supervised and not left alone with children.

Not in scope:

- preschool aged children who attend an early learning program in a school setting integrated with the first years of school'
- schools (except school-based preschools)
- school buses
- out of school hours care
- Family Day Care educators.

Note: FDC educators must comply with the Family Day Care Safe Use of Digital Technologies and Online Environments Operational Guide.

3. Contents

4. Detail

Children and young people have a right to safety and protection at all times, including when being photographed or filmed and when accessing electronic devices and technologies at department ECEC services and programs.

This policy is part of the department's obligations and commitment to safeguard and promote the wellbeing of children and builds on the responsibilities and obligations of individuals and ECEC services and programs outlined in the safeguarding children and young people policy (PDF 668 KB).

The safety and wellbeing of children remains a priority for all levels of government and is a key objective of the National Quality Framework (NQF). On behalf of the Australian federal government and all state governments, the Australian Children's Education and Care Quality Authority has undertaken a review of child safety arrangements under the NQF. Following the review, a voluntary National Model Code for Early Childhood Education and Care (PDF 95 KB) was developed to support providers and services to promote a child safe culture. In response to the review a number of regulatory amendments were made to strengthen requirements for child safety in policy.

This policy meets the requirements of regulation 168 of the Education and Care Services National Regulations and delivers on the department's commitment to the National Model Code for Early Childhood Education and Care and the South Australian prohibition on the use of personal mobile devices in ECEC services and programs.

The policy is complemented by the protective practices for staff in their interactions with children and young people guidelines for staff working or volunteering in education or care settings (PDF 3 MB) which provides clear advice to adults for the establishment of positive, safe and respectful relationships with children and young people in education and care settings, and to support staff to feel confident about meeting their responsibilities to children and young people as well as their professional ethics and conduct obligations.

Any breach of this policy is to be immediately reported to the site leader. The site leader is to manage any incident in accordance with their responsibilities outlined in managing and responding to employee misconduct (staff login required).

4.1. Electronic devices

4.1.1. Personal electronic devices that can take images and video

All staff and volunteers working with or providing a service to children at department ECEC services and programs are not permitted to have a personal electronic device that can take images or videos (such as mobile phones, digital cameras, tablets, smart watches and other new and emerging technologies, where those technologies have image taking or video recording capability), in their possession or with them when:

- they are working directly with children, whether indoors or outdoors, on an excursion or transporting children
- they are in a space or spaces that are primarily used for ECEC services or programs.

Staff and volunteers must ensure their personal electronic devices are appropriately stored in areas away from spaces used by children such as in a staff room or office. Parents who are interacting primarily with their child are able to retain their personal electronic devices for example picking up and dropping off their children, playgroup etc but must not use personal electronic devices for taking images except of their children. Parents are encouraged to refrain from using personal electronic devices in ECEC services and programs.

There are limited exceptional circumstances where staff or volunteers may seek approval in writing from the site leader or Education Director as appropriate to be in possession of a personal electronic device for an essential purpose where that access does not impede the active supervision of children, including:

- personal health requirements (such as heart or blood sugar level monitoring)
- disability (such as where a personal electronic device is an essential means of communication for an educator or staff member)
- family necessity (such as a worker with an ill or dying family member).

Written approval must be obtained before the staff or volunteer is permitted to be in possession of a personal electronic device when working with children. Such approval is given for the essential purpose only and the personal electronic device must not be used for any other purpose including taking images and videos of children.

There may be emergency circumstances where a site leader may need to provide once off written approval for staff or volunteers to possess a personal electronic device for an essential purpose when working with children. Circumstances may include:

- lost child, injury to child or staff member, other serious incident, or in the case of a lockdown or evacuation of the service premises
- technology failure (such as when a temporary outage of service issued electronic devices has occurred)
- local emergency event occurring to receive emergency notifications through government warning systems (such as bushfire evacuation text notification).

Such approval is given for the essential purpose on that occasion only and the personal electronic device may not be used for any other purpose.

4.1.2. Service issued devices

Only service issued devices are to be used to take images and videos of children. Service issued devices are those that are provided by the department to employees where their manager makes an assessment that they require an electronic device for their work. Service issued devices are assets of the site and should be included in the site asset register.

Through the Preschool Uplift Program (PUP) department preschools have received an allocation of approved electronic devices to support administration, communication and teaching and learning programs. The cost of purchasing additional devices are to be met within the available resourcing of the service in line with

department procurement policies and arrangements (staff login required). Any devices provided or purchased through the department and then issued to staff are also considered service issued devices.

Wi-Fi enabled service issued devices must use a department provided sim card or wireless service from an approved supplier in line with department procurement processes and arrangements. Services must ensure purchase of sim cards or internet services are consistent with the ICT cyber security standard (PDF 1 MB).

The department's ICT cyber security standard (PDF 1 MB) outlines requirements about using and managing service issued devices including mobile phones, tablets, USB drives, external hard drives, and laptops.

The following must be observed with respect to the use of service issued devices on the preschool or department network:

1. Only service issued devices owned or operated by preschools or the department may be used to connect to department infrastructure or services
2. Service issued devices must not be used by an employee's family or friends
3. USB thumb drives or portable drives from an unknown or untrusted source are not to be connected to department equipment.

All staff accessing the corporate network are required to read and sign the ICT Acceptable Use Agreement which includes information on the acceptable use of ICT resources, and consequences of inappropriately using department assets.

4.2. Images and videos of children

4.2.1. Consents from parents to take, use and store images and videos of children

ECEC services and programs must obtain consent from parents to take, use and store images and videos of children. Consent must be in line with the department's expectations when using image, video, voice, performance or creative work of children as per the consent to use media and creative works procedure (PDF 192 KB). Consent will be sought upon enrolment. Consent may be revoked by a parent or carer at any time.

4.2.2. Taking images and video of children

When used intentionally as part of implementing an educational program, electronic devices can be a useful educational tool, including to assist in documenting a child's learning. Services should be clear about their purpose for taking images of children and must ensure appropriate practice when taking images and videos of children. Where possible, images should only be taken in places where another educator or staff member can see the image being taken.

ECEC staff can only take and access images and videos of children on service issued devices. Taking images of children must primarily relate to children's learning, development and wellbeing and include taking active steps to ensure the safety, privacy, dignity and rights of individuals.

Prior to taking images and video, appropriate consents from parents must be obtained and respected. Due consideration should also be given to ascertaining children's assent to be photographed or filmed. This includes verbal or non-verbal assent such as smiling or nodding (to assent) or shaking head, turning away (showing dissent).

When at the service, parents may take images of their own children but must not take images of any other children including where their own child is part of a group, for example an end of year concert or sports day.

Only ECEC staff are permitted to take images and videos of children. If work placement students and educators on practicum are required to take photos or video of children as part of their studies, additional written permission must be obtained by from parents or carers and images must be taken by a staff member using a service issued device with the permission of the site leader.

4.2.3. Inappropriate images or videos of children

Inappropriate images and videos of children must not be taken.

Inappropriate images or videos are any that do not directly relate to the individual child's participation in activities in the education and care program including where a child is:

- not appropriately dressed or in a state of undress including in their underwear or where genitalia are exposed
- toileting or having their nappy changed
- in a pose or position that could be perceived as sexualised
- anxious, in distress, or experiencing or demonstrating dysregulation
- compromised in regard to dignity or cultural background
- injured and first aid has not yet been administered.

4.2.4. Using images and video of children

Digital photos and videos have become a common tool in ECEC services and programs. This type of communication can and does play a role in engaging families in a child's education and care experiences, particularly where there may be low levels of literacy or English is not a family's first language.

As part of consenting to their child being photographed and videoed, parents should also be made aware of how images will be used by the service including:

- creating identity and belonging through photo displays of individuals and groups in the service
- identifying children with additional support, health or medical requirements
- documenting and sharing children's learning and engagement
- informing and supporting assessment and reporting on children's learning
- communicating with families about their child's participation in the learning program.

Services may use a range of applications such as Class Dojo and See Saw to share images with parents. It is important that sites consider the purpose and frequency of sharing images via these channels and achieve an appropriate balance between the primary responsibility of educators to engage, interact and supervise children in their learning, and communication with families.

Use of applications should be restricted to parents of children currently enrolled in the service. Invitations should not extend beyond these boundaries. Access to the app should end when the child ceases enrolment at the service.

From time to time, services may use images of children in external promotion activities including social media. Consent for public activities beyond the service, must be in line with the consent to use media and creative works procedure (PDF 192 KB) and webpage (staff login required).

It is inappropriate for any image or video of a child to be shared to platforms beyond the intended purpose of the image or video, or for which permission has been obtained.

4.2.5. Storing images of children

Data privacy and security play a crucial role in protecting personal and sensitive information in the digital world. Data privacy focuses on the proper handling and use of personal or sensitive information. Data security focuses on the protection of digital information from unauthorised access, disclosure, alteration, or destruction.

Images of children should only be accessed and stored on service issued devices. Digital images and video must not be shared or downloaded to other devices and platforms that are not approved or monitored by the service.

Personal storage and file transfer media such as SD cards, USB drives, hard drives and cloud storage should not be in the possession of, or available to, any staff member or volunteer while providing education and care and working directly with children.

Service issued devices are not to be used as the sole repository for department information. All department information stored on service issued devices must be regularly backed up to an appropriate network location, cloud service, or application intended and approved for storing official information.

Officers from ICT Services will provide guidance, upon request, on user responsibilities and options in relation to data back-up for important information that is stored locally. These back-ups must be given adequate protection against theft or loss.

4.2.6. Destruction of images

Under the Department of the Premier and Cabinet Circular PC 012: Information Privacy Principles (IPPS) Instruction, the ECEC service or program will take reasonable steps to ensure that personal information in its possession or under its control are securely stored and not misused.

The information and records management for schools and preschools procedure (PDF 187 KB) outlines the process for managing preschool records from creation to disposal, including digital records, in line with legislative requirements under the State Records Act 1997. The school and preschool official records

webpage (staff login required) provides further advice on official records and how to manage them, including the Operational Records Disposal Schedule (PDF 501 KB).

Corporate staff should refer to the information and records management for corporate office procedure (PDF 224 KB).

4.3. Optical surveillance devices

4.3.1. CCTV

Optical surveillance devices such as CCTV can be used as a site security measure to assist with the following:

- The protection and safety of children and staff
- The prevention and detection of crime
- The protection and security of physical assets

CCTV must not be viewed as a replacement for effective, active supervision of children by educators.

In ECEC services and programs, CCTV brings important ethical implications including privacy concerns and the appropriate purpose of obtaining, using and storing the footage. ECEC services and programs that intend to use CCTV internally must undertake extensive consultation prior to installation. As part of the consultation, information must be provided on the intended purposes of the footage, the locations of the cameras and how the footage will be stored and accessed. The following should be consulted:

- Parents of children who attend the site
- Staff that work at the site
- School Governing Councils or Preschool Management Committees
- The Industrial Relations & Policy Directorate

In addition to the above, the Security and Emergency Management (SEM) Unit must be contacted for advice, support, and approval for CCTV installation to ensure compliance with the department and legislative requirements. The placement of cameras internally must also be reviewed and endorsed by the Agency Security Advisor within the SEM unit.

4.3.2. Sleep monitors

Sleep monitors in cot rooms may act as a supplementation to visual monitoring of children when asleep or rest; however, such monitors must not replace regular physical checks and in-person supervision as required by the safe sleeping and resting for infants and young children policy (PDF 580 KB).

The connection of sleep monitors to wireless networks adds an additional privacy risk because of the increased possibility of data being intercepted by people using electronic hacking devices. It is recommended that ECEC services and programs consider purchasing sleep monitors that only show live feed or sound and do not store images.

If a service uses a Wi-Fi enabled sleep monitor it must ensure that security controls, including password protection and the storage of images, are consistent with ICT cyber security standard (PDF 1 MB).

4.4. Digital devices used by children

The use of digital technology in ECEC services and programs sits within a broader learning environment that is play based, where children's learning is dynamic and holistic and where children are active participants in their learning. The early years learning framework (EYLF) outlines that 'digital technologies and media can enable preschool children to access global connections and resources and encourage new ways of thinking'. This includes children using digital technologies and media to investigate and problem solve.

Digital devices in ECEC services and programs are primarily a teaching and learning tool used by educators and not a device for passive consumption by children, for example integrating the use of technologies into children's multimodal play. The Australian Government has published physical activity guidelines by age which set out recommendations for the maximum amount of screen time for children. Children aged 3 to 5 should have no more than 1 hour of screen time per day which includes use at home.

All devices must only be used by children when they are actively being supervised. Educators must be able to observe screens directly, monitor children's online activities and respond promptly to any signs of unsafe behaviour or distress.

Additionally, educators will need to develop risk assessments with children regarding the use of digital technology and online environments. The risk assessment will include online safety, including steps for notifying educators of anything unsafe or inappropriate on the device when they use it and the environment in which they are to use the device.

Where children in ECEC services and programs access digital devices their use must be:

- be part of the teaching and learning program
- appropriate to the age of the child
- strictly time limited
- modelled and supervised by an educator in shared spaces
- supportive of healthy posture to avoid strain when looking down at devices

Digital devices for children in ECEC services and programs must:

- be service issued
- have strong privacy settings enabled

Digital devices for children in ECEC services and programs must not:

- provide unrestricted and/or unsupervised access to the internet
- enable any personal information, including images, to be uploaded
- be used as a strategy to manage children's energy, engagement or behaviour
- be used as a response to weather conditions

- use free apps that pose risks to pop up advertisements and inappropriate content
- pose risks to children's physical health and wellbeing through overuse, strain or eye glare.

Children in ECEC services and programs should not bring digital devices from home including smart watches and air tags. The site leader may approve the use of digital devices for educational or communication purposes such as an augmented and alternative communication device (AAC) for a child with additional needs/disability.

4.4.1. Use of AI and emerging technologies

Technology is constantly evolving, as is the way our communities, families and children interact with it. AI is now part of many digital experiences, offering both opportunities and new risks.

Like many digital technologies, AI-enabled technologies must be used with careful consideration of data privacy and security risks. This is important because these technologies are reasonably new, complex and currently unregulated.

The department has developed EdChat (staff login required) which is a generative AI chatbot. It is custom-built for teaching and learning and is tailored to public education in South Australia. EdChat has extra safety features that improve data security and prevents access to inappropriate content compared to openly available AI chatbots such as ChatGPT.

Where an AI tool is to be used by educators in ECEC services and programs EdChat is strongly recommended. EdChat, has unique guardrails for protecting data and privacy and all responses remain the property of the department rather than a third party.

When using EdChat it is best practice that staff do not share any personal or identifying information about children or the site including images, videos, name, address, sensitive information or health information. Educators must not enter any personal or identifying information about children or the service including images, videos, name, address, sensitive information or health information into any other AI tool.

The use of EdChat and any other AI tool is age restricted and generally not suitable for preschool aged children unless part of a recognised program, such as those focusing on STEM (science, technology, engineering, and mathematics) or early language development.

5. Roles and responsibilities

5.1. Executive Director, Preschools and Early Childhood Services

Has approved provider responsibilities under the Education and Care Services National Law and Education and Care Services National Regulations.

5.2. Quality Preschools Directorate

Monitor, review, and evaluate the effectiveness of this policy in accordance with the department's operational policy requirements.

Provide advice and support to department staff about the application of this policy.

5.3. Education Director

Ensure principals and preschool directors develop a site-specific procedure, implement this policy and any associated procedures.

In exceptional circumstances approve in writing the possession of personal electronic when working with children for a Principal or preschool director.

5.4. Education Lead, Early Childhood

Provide support and advice to principals and preschool directors to interpret this policy.

5.5. Long day care management committees and school governing councils with a school-based preschool

Ensure all staff and volunteers comply with this policy and any associated procedures.

5.6. Principal or Preschool Director

Comply with this policy and must develop their own local procedure for the safe use of digital technologies and online environments.

Report any breach of this policy in accordance with employee misconduct which may include a notification in the department's incident management system.

In exceptional circumstances approve in writing the possession of personal electronic when working with children.

5.7. Staff, volunteers and contractors

Comply with this policy and any associated procedures.

5.8. Visitors

Agree in writing that they will not take any images or videos of children whilst at the ECEC service or programs.

6. Definitions

6.1. early childhood education and care service

Department's education and care services and programs delivering ECEC to children including:

- children's centres
- crèche
- occasional care
- integrated services with long day care programs
- learning together communities
- playcentres
- playgroups
- preschools including school-based preschools
- rural care
- Note: Schools, school buses, Family Day Care educators and Out of School Hours Care are not in scope of this policy.

6.2. personal electronic device

Any device that can take images or videos (such as mobile phones, digital cameras, tablets, smart watches and other new and emerging technologies, where those technologies have image taking or video recording capability) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage). Any images taken with any camera, including non-digital, is in scope of this policy.

6.3. service issued device

A laptop, notebook, tablet or mobile phone that uses wireless/mobile telecommunications technology provided by the education and care site, service, program or department for the use of staff/employees for work related activities.

6.4. parent

For the purposes of this policy, the term 'parent' refers to all persons responsible for the child. A person responsible for the child means a person who is the child's:

- biological parent, adoptive parent or other person recognised as a parent if the child was conceived following a fertilisation procedure or under a surrogacy arrangement
- guardian

- person standing in loco parentis.

This does not include a person who has had their legal custody, guardianship or responsibility for the child removed by a Court, Act or Law. As an example, a biological parent who has had their custody, guardianship or parental responsibility for the child removed by a parenting order made under Family Law Act 1975 (Cth) is not a person responsible for the child.

6.5. visitor

A person who is not listed as being in scope of this policy and is not a parent of a child enrolled in the ECEC service or programs. A visitor may include, but is not limited to, visiting allied health professionals, employees or contractors for other government agencies, contractors employed by third party providers (such as Ventia) and children's performers and entertainers.

7. Supporting information

ACECQA: National Model Code for Early Childhood Education and Care – Taking images or videos of children while providing early childhood education and care (PDF 95 KB)

ACECQA: NQF Online Safety Guide (PDF 7 MB)

ACECQA: Policy guidelines – Safe use of digital technologies and online environments (PDF 241 KB)

Managing and responding to employee misconduct (staff login required)

Template for safe use of digital technologies and online environments procedure (to be developed)

7.1. Related legislation

Education and Early Childhood Services (Registration and Standards) Act 2011 (including schedule 1, Education and Care Services National Law (South Australia))

Education and Care Services National Regulations

7.2. Related policies

Culturally Responsive Framework (PDF 10 MB)

Protective practices for staff in their interactions with children and young people guidelines for staff working or volunteering in education or care settings (PDF 3 MB)

Safeguarding children and young people policy (PDF 668 KB)

Selecting and using resources for educational purposes guideline (PDF 626 KB)

8. Record history

Published date: September 2025

8.1. Approvals

OP number: 349
File number: DE25/21665
Status: approved
Version: 1.0
Policy Officer: Senior Leader, Preschool Policy and Advice
Policy sponsor: Director, Quality Preschools
Responsible Executive Director: Executive Director, Preschools and Early Childhood Services
Approved by: Executive Director, Preschools and Early Childhood Services
Approved date: 29 August 2025
Next review date: 29 August 2028

8.2. Revision record

Version: 1.0
Approved by: Executive Director, Preschools and Early Childhood Services
Approved date: 29 August 2025
Review date: 29 August 2028
Amendment(s): New policy.

9. Contact

Quality Preschools

Email: education.NQFChildSafety@sa.gov.au