Safe use of digital technologies and online environments procedure

Purpose

This procedure details how we meet our commitment to child safe practices for digital technologies and online environments.

Background

This procedure addresses the requirements in regulation 168 which require an education and care service to have policies and procedures for the safe use of digital technologies and online environments, including the use of mobile devices.

Children and young people have a right to safety and protection at all times, including when being photographed or filmed and when accessing digital devices and technologies at Avenues College Children's Centre.

This procedure 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 early childhood education and care (ECEC) services and programs outlined in the Safeguarding Children and Young People Policy.

A copy of this procedure will be kept in the Policies and Procedures folder in the entrance to the preschool learning environment and on our website. It is also available upon request.

Legislative requirement

In relation to the safe use of digital technologies and online environments, the National Regulations requires services to have policies and procedures for the safe use of digital technologies and online environments (regulation 168).

This procedure outlines how Avenues College Children's Centre will implement the Safe use of digital technologies and online environments policy.

Procedures

Electronic devices

Personal electronic devices that can take images of children

Employees and volunteers (including work experience students) working with and/or providing a service to children at this service are not permitted to have a personal electronic device in their possession that can take images when:

- they are working directly with children
- they are in a space or spaces that are primarily used for children's programs or services when children are in attendance.

Employees and volunteers, outside of the preschools approved premises, who are not directly working with or have responsibility for preschool children, can retain their personal electronic devices, however they must not take images of preschool children.

Personal electronic devices will be stored in personal lockers or in bags inside the staff learning space.

Staff and volunteers can use their personal electronic device when on breaks in a space not used for children's programs or services including the staff learning space, Preschool Leader's office and within the school environment, outside of the preschool.

Smart watches or any other device that does not have the capability to take images or videos can be worn at the service. This will be discussed at induction, when documentation will be signed related to agreements regarding safe use of digital devices.

There are limited exceptional circumstances where an employee or volunteer may seek approval in writing from the site leader to be in possession of a personal electronic device which can take images or video including health needs, disability or urgent pressing necessity.

Where a staff member or a volunteer believes their circumstances constitute exceptional circumstances, they can complete the Exemption request – on site possession of a personal electronic device application form for consideration by the site leader. If approval is granted it will be for the stated essential purpose only and the personal electronic device must not be used for other purposes.

Exceptional circumstances applications will be considered on a case by case basis and the criteria for any approval will be consistent with the Safe use of digital technologies and online environments policy and the National Model Code and Guidelines.

In emergency circumstances such as a child is lost or missing or the site is in lockdown the site leader may give one off approval for educators to use their personal electronic devices. All approvals and details of the device will be recorded on the essential once-off approvals register after the event.

For regular outings, or where children are being transported on the preschool bus, the site leader may approve a staff member or volunteer to have their personal device in their possession for child safety or emergency purposes. The site leader will record this approval and details of the device on the essential planned approvals register. No images or videos of children may be taken on personal devices, and the device can only be used for the approved purpose.

Where staff or volunteers provide emergency contact details such as their child's school or next of kin, staff and volunteers are encouraged to share the services landline number, or service issued mobile device number.

Parents will be discouraged from using their personal electronic devices when in attendance at the service. This information will be communicated to parents during orientation and through our online platform. The Procedure will also be shared on the site's website. The personal device free area poster is also prominently displayed for visibility.

Posters will be displayed in the entrance to the preschool, alongside of the prescribed information, in the children's learning areas and near the community space to alert families and visitors of the ban on taking photos or videos of children.

Service issued devices

At our service, only service issued devices are to be used to take and access images and videos of children. All educators who need digital devices in the course of their work will be provided access to a service issued device at the discretion of the Preschool Leader or Principal. To utilise a shared Windows device, staff members must log in using their EdPass user account or local domain account. For shared iPads, staff members must sign in and out of the necessary applications as needed.

All staff must read and understand the Department for Education's ICT cyber security standard and sign the ICT Acceptable Use Agreement declaration and complete PLINK Cyber Security Training Course before using service issued devices.

The site leader will maintain a record of all service issued or borrowed devices.

Service issued devices which are used by staff and volunteers for taking, sharing or storing images or videos of children and/or used in programs with children must not be used for personal use.

Images and videos of children

Consent from parents to take, use and store images and videos of children

We will obtain parental consent before taking, using, distributing or storing images and videos of their children.

At the time of enrolment parents will be asked to complete the consent to publish media and creative work of children, students and the community. The consent forms will be stored with the child's enrolment record in accordance with the department's Information and records management requirements .

If parent permission is revoked, every effort will be made to remove relevant media from distribution, however this may not be possible or practical in some situations.

Taking Images and videos of children

We believe:

- electronic devices are a useful educational tool to document children's learning
- digital images and videos play an important role in engaging parents in their child's education and care experiences
- provide a valuable way of sharing the cycle of planning and our learning design with families.
- digital devices support connection with families beyond the physical preschool environment.

We will:

- only take images or videos on service issued devices
- seek children's consent before taking images or videos
- ensure children's privacy, dignity and rights are respected
- where possible another educator or staff member will be present when images are taken.
- continue to critically reflect on our use of digital images to ensure that images or videos relate directly to children's learning, development and wellbeing.
- be intentional in our approaches to documentation of children's learning.
- ensure we prioritise active supervision, interactions and engagement with children in their learning.

Parents of children enrolled in our service and programs will be discouraged from using their personal electronic device while at the service, noting they will not be prohibited from taking an image of their own child, but must not take images of other children, including where their child is part of a group.

Staff will communicate to parents the importance of child-safe environments and explain how the service is implementing the newly introduced regulations to enhance child safety.

If a parent takes images of children, other than their own, we will request that they stop taking images and delete any taken images. If the request is ignored, or the parent becomes offensive or abusive the site leader will lodge a critical incident report. If required we will contact Conditions for Learning directorate if urgent assistance is required.

Before being granted access to the service visitors, including maintenance contractors, will be asked to agree, as a condition of entry, that they will not take images or videos of children by completing the visitor sign in register.

Visitors including maintenance, contractors may, with the site leader's or delegates permission, take images for approved purposes, such as taking images of site infrastructure to obtain a quote.

Work experience students and volunteers must not take images and videos of children.

Where images are required as part of a practicum, additional consent will be obtained from the parent and approval sought from the site leader. Images will be taken on a service issued device by a staff member and the student provided a hard copy of the image.

Inappropriate images and videos of children

Our service will take active steps to ensure the safety, dignity and the rights of a child are respected when taking images or videos and not take any inappropriate images or videos of children. Refer to Safe use of digital technologies and online environments policy for more information.

Educators and volunteers must not take or use service issued devices in children's bathrooms or nappy changing areas.

Parents will be discouraged from sending inappropriate digital images of their child to the service, for example eg photos of a child's nappy rash or injuries. This information will be communicated through our handbook, during orientation visits and on the website.

Using images and videos of children

We use the Compass platform images with families in line with parental consent.

We use images to:

- create identity and belonging through photo displays of individuals and groups of children
- identify children with additional support, health or medical requirements to support child safety
- document and share children's learning
- inform and support assessment and reporting
- communicate with families about their child's participation in the learning program

Staff will only distribute messages and content to parents using service issued devices and only to parents of children currently attending the service, who have given required consent.

Storing images of children

In accordance with the Safe use of digital technologies and online environments policy we will only download, access, share or store images or videos using service issued devices on platforms supported and approved by the department, such as Frog, cloud storage or the sites network in accordance with the ICT cyber security standard.

We ensure that all department official records are regularly backed up onto Microsoft Teams, which are approved by the department for the storage of information. These will be backed up by each individual educator responsible for the device allocated. This will be conducted weekly, with images deleted from the device following the completion of this process.

All records will be stored in accordance with the Identifying, creating and managing official records webpage and the Information and records management for schools and preschools procedure.

Staff will not use personal storage and file transfer media such as SD cards, USB drives, hard drives or cloud storage to save or store images or have them in their possession while working directly with children.

[add any additional site-specific information here for example a school-based preschool may wish to provide the contact details of their ICT person for further guidance].

Destruction of images

All digital records at our site, from creation to disposal, will be managed in accordance with the School and preschool official records webpage and the Information and records management for schools and preschools procedure.

For additional security reasons an identified staff member will be responsible for transferring children's images and videos from portable digital devices to the sites record management systems (Microsoft Sharepoint/Teams)

The site leader is responsible for ensuring that all records are archived or disposed of securely in accordance with the Operational Records Disposal Schedule at the end of each preschool or school year.

Optical surveillance devices

CCTV

CCTV is used at our site as a 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.

Installation, storage and access of CCTV images and data

Our CCTV systems are professionally installed and maintained in accordance with the department standards, the South Australian Surveillance Devices Act 2016 and legislative requirements.

We have signage indicating the presence and operation of CCTV cameras and recording equipment as appropriate to the location of the camera installation.

Cameras are not placed in locations or in such a manner as to significantly infringe upon the private activity of any persons lawfully attending or utilising this site or facilities.

For privacy reasons cameras are not located in Preschool, children's bathrooms, nappy change or toilet areas.

Access to CCTV footage at the service is strictly controlled and protected by secure, password-protected systems and only authorised personnel are permitted to access the footage.

All CCTV footage is an official record for the purposes of the *State Records Act 1997 (*SA) and will be dealt with and managed in accordance with the provision of the Act.

The site leader will ensure:

- only the following authorised persons can access CCTV system and footage(Nominated Supervisor, responsible person and ICT support personnel).
- all persons authorised to access the video management software have an individual login and password to enable auditing and logging of persons accessing footage.
- CCTV footage is stored on a secure storage server for a period of up to 31 days. Any recorded footage will be destroyed or de-identified when it is no longer needed for the purpose it was collected.
- CCTV footage will not be accessible to external parties (e.g. other staff members or families) without appropriate authorisation.

Following a critical incident the site leader will:

- determine whether there is CCTV footage of the alleged incident.
- immediately report any issues, incidents or security concerns using the department's incident management system in accordance with the Reporting critical Incidents, injury and hazards and near misses procedure. The report should specify if there is any CCTV vision of the incident.

- liaise with the Education Director, Incident Management Division (IMD) and the Regulation and Compliance team in Preschools and Early Childhood Services (PECS) for advice and support as required.
- immediately contact South Australian Police (SAPOL) on 131 444 if any suspected criminality, such as assault or child sexual offending.
- contact IMD for advice if the matter relates to possible educator misconduct.
- only release CCTV footage to authorised entities, such as SAPOL, Education Standards Board (ESB), or other law enforcement agencies.
- seek advice from IMD or the Regulation and Compliance team regarding any authorised requests for CCTV footage.

Digital devices used by children

Our service believes the use of digital technology 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.

Early Childhood Australia's statement on young children and digital technologies guides our reflection on children's use of digital technologies including considering how digital technologies enhances children's:

- relationships with others
- health and wellbeing
- citizenship and online privacy
- learning through play and intentionality.

We also refer to selecting and using resources for educational purposes guideline for considerations about the appropriateness of children's use of digital resources within the preschool program.

Educators will limit children's screen time in line with Australian Government physical activity guidelines by age, which set out recommendations for the maximum amount of screen time for children.

Physical Activity Guidelines

Age of child	Recommended screen time
birth to 24 months	No screen time
24 months to 5 years	Less than one hour a day
5 – 12 years	For entertainment no more than 2 hours a day.

When children are accessing digital technologies and online environments educators will ensure:

- digital devices are integrated as part of the learning program
- programs and software children can access and use are age appropriate
- they vet children's use of social media platforms carefully to avoid inappropriate content, including YouTube
- all new apps and games are checked for age and developmentally appropriate content before they are used
- children only access digital technologies in shared spaces and are actively supervised at all times
- where possible they remain in line of sight of other staff members when working with children

- they model the safe use of digital technologies and online environments
- screen time is strictly limited
- they model appropriate use of the internet and software programs
- children are encouraged to use their protective behaviour strategies when feeling unsafe, for example tell a staff member or a trusted adults if they encounter anything that makes them feel uncomfortable, scared or upset

Educators will not:

- provide unrestricted and unsupervised access to the internet and digital devices
- upload personal child information or images to AI tools except EdChat
- upload images or video of children to EdChat on personal devices
- use digital devices as a strategy to manage children's energy, engagement or behaviour
- use digital devices in response to weather conditions
- use free apps that pose risks to pop up advertisement and inappropriate content
- place digital devices in areas where educators cannot monitor their use
- pose risks to children's physical health and wellbeing through overuse, strain or eye glare

Children bringing personal electronic devices from home

Due to safety and security risks parents are requested not to bring children's digital devices from home including smart watches and air tags.

This information will be communicated to families at the time of enrolment through orientation processes including our handbook and enrolment connections.

The site leader may approve the use of children's digital devices from home for educational or communication purposes such as an augmented communication device (AAC) for a child with additional needs or disability. Parents will be encouraged to discuss their child's learning needs and any special considerations at the time of enrolment.

If approval is given for a child to have a digital device, approval will be recorded on the child's enrolment record, EMS and a log sheet and may be time limited. If approval is time limited a parent who is seeking an extension will be encouraged to make an appointment with the site leader to discuss their child's learning needs.

The site leader will check with parents to ensure appropriate parental controls and restrictions are in place on any digital device bought from home to ensure children's safety prior to it being brought to the service.

Working with parents and the community

We believe that parents are children's first and most important teachers. We will work in collaboration with parents to support and promote children's safe use of digital technologies and online environments including:

- consulting with parents, staff, Aboriginal Elders and community knowledge holders about culturally appropriate and safe content
- working with parents to ensure appropriate parental controls and restrictions are in place to ensure online safety on any approved child devices brought from home
- encouraging parents to talk to their children about online risks in an age and developmentally appropriate way (see useful resources below)

- sharing information with parents about recommended screen time limits in accordance with the Australian Government physical activity guidelines
- parents will be informed if their child has accessed digital technologies to ensure families can manage screen time.
- promoting the availability of useful resources for parents about online safety through our newsletters, social media, website and parent handbook.

Useful resources

Online safety support – Department for Education

how to choose good online content – eSafety Commissioner

Media & technology for preschoolers – Raising Children Network

Induction of staff and volunteers

All staff and volunteers including work experience students will have current Responding to Risks of Harm, Abuse and Neglect – Education and Care (RRHAN-EC) training before commencing at the site to ensure they understand their role and responsibilities in safeguarding children.

As part of the service induction process all staff and volunteers including work experience students will have ready access to the Safe Use of digital technologies and online environments policy and this procedure including staff and volunteers who don't usually work directly with or have responsibility for preschool aged children in ECEC services or programs.

All staff, volunteers and work experience students will be expected to read, understand and adhere to the Safe Use of digital technologies and online environments policy and this procedure including staff and volunteers who don't usually work directly with or have responsibility for preschool aged children in ECEC services or programs.

Staff and volunteers will be supported to access relevant training relating the safe use of digital technologies and online environments including access to relevant Plink online training.

Online Safety

Our site will implement the Responding to online safety incidents in South Australian schools guideline in response to any incidents of inappropriate or risky online behaviour by children or adult behaviour targeted at children.

For online safety incidents that involve allegations of staff member misconduct our educators will be guided by the following documents:

Protective practices for education and care staff and volunteers

Responding to online safety incidents in South Australian schools guideline

Child protection policies and guidelines

The site leader will also report any incidents on the department's incident management system in accordance with the Reporting critical incidents, injuries, hazards and near misses procedure.

Use of AI and emerging technologies

Educators at our site are encouraged to use EdChat, the department's secure generative artificial intelligence (AI) chatbot as the preferred tool due to its additional safety features. Due to its additional security controls staff can enter personal or identifying information about children or the site such as images, videos, names, addresses, or health information.

If educators are using EdChat on a personal device, they are unable to upload images and videos of children.

We will adhere to the Artificial intelligence in schools – use and considerations guidelines before approving the use of any other AI tools. If alternative tools are approved, staff will not enter any personal or identifying information about the site or children. This includes uploading images or video of children.

If educators are using AI to help with programming and creating learning experiences this will not be done where children are present.

We will limit the use of AI with children to recognised programs such as those focusing on STEM or early language development. Any programs will be age-appropriate, safe and aligned with the principles, practices and learning outcomes described in the Early Years Learning Framework. Educators will ensure children will be closely supervised when accessing tools and toys with AI capability to ensure privacy and data security is maintained.

Procedure creation and revision record

Version:	2
Approved by site leader:	Hamish McDonald
Date of approval:	26/03/2026
Date of next review:	March 2029
Amendments(s):	Nil