C.a.F.E. Enfield Children's Cente

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 C.a.F.E. Enfield 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 policy folders located in the Centre foyer and preschool verandah. The procedure can also be access on the policy page of our website.

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 C.a.F.E. Enfield 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.

Whilst children are attending the service.

Personal devices such as phones, tablets and smart watches belonging to staff and students who work directly with children must be stored in staff lockers.

They can be accessed during break and meal times only in a space not used for children's programs or services including the staff room, office areas, meeting rooms or community space garden.

External service providers who come on site to work directly with children must either leave their personal devices in their car or in a lock box in the admin office whilst working with the children or in spaces used by children.

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 Director. 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 will be recorded on the Emergency circumstances – register of approvals after the event.

Where staff or volunteers provide emergency contact details (for example to their child's school) they are encouraged to share the Centre's landline number so that they are able to be contacted in an emergency.

Parents will be discouraged from using their personal electronic devices at the Centre. This information will be communicated to parents in the parent handbook and during orientation visits.

Service issued devices

Only service issued devices are to be used to take and access images and videos of children. The Centre provides each room with ipads for the purposes of taking images or videos of children to support documentation of children's learning and development.

To use our Centre computers, staff members must log in using their EdPass user account

For shared iPads, staff members must sign in with a code to access 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 Centre has a mobile phone which is permitted in children's rooms for the purpose of making/ taking phone calls from parents when required.

The site leader will maintain a record of service issued devices in the Centre asset register..

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 departments 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 the intentional use of digital images and video are effective tools to:

- document children's learning
- engage parents in their child's learning and development
- support educators' understanding of children, critical reflection and professional development
- At our Centre we have made a conscious decision not to use social media for communicating with families. We do not use app-based programs for sharing documentation or photographs. This is for a range of reasons including maintaining children's safety and rights regarding digital images, it is also to encourage educators to be present with children and engaging in more purposeful forms of documentation of children's learning.

We will:

- only take images or videos on service issued devices
- endeavour to seek children's consent before taking images or videos
- ensure children's privacy, dignity and rights are respected
- be intentional in our approaches to documentation of children's learning.
- 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.

- ensure we prioritise active supervision, interactions and engagement with children in their learning.

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.

Parents & family members of children enrolled in our service and programs will be discouraged from using their personal electronic device while in the children's rooms, outdoor playspace or at playgroups.

At Centre events and celebrations we ask that parents & family members do not take photographs , or video.

If a parent/ family member takes images of children 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 and 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 and 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.

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, in a state of undress, or whilst distressed]. This information will be communicated via the parent handbook

Using images and videos of children

We use images to:

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

Staff will only distribute messages and content to parents (via email or paper copy) 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 to the Department for Education cloud based infrastructure which are approved by the department for the storage of information. This is an automatic 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.

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.

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

Sleep Monitors

- We ensure that all children are provided with safe sleep and rest at our site in accordance with the department's Safe sleeping and resting for infants and young children policy and Safe sleeping for infants and young children procedure.
- Our service uses sleep monitors in cot rooms as a supplementation to visual monitoring of children when asleep or resting. The monitors do not take the place of regular checks and active supervision as required by the Safe sleeping and resting for infants and young children policy and our safe sleep and rest procedure
- Our sleep monitors **only use live feed**, and no images of children are stored on sleep monitors.

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 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 children	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 behaviours 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 including EdChat and ChatGPT
- 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 the parent handbook.

The site leader may approve the use of children's digital devices from home for educational or communication purposes such 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 One Plan, Autism Spectrum Support Plan or Health Support Agreement (as applicable) 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
- 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 services 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.

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.

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

If educators use AI as part of their work (Eg programming),they are encouraged to use EdChat, the department's secure generative artificial intelligence (AI) chatbot as the preferred tool due to its additional safety features. When using EdChat, staff **will not** share any personal or identifying information about children or the site such as images, videos, names, addresses, or health information.

We will follow the Artificial intelligence in schools – use and considerations before our service approves the use of other AI tools. If alternative tools are approved staff will not enter any personal or identifying information about the site or children.

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

Procedure creation and revision record

Local procedures must be regularly reviewed and maintained to ensure they remain relevant and up to date with important developments in evidence-based practices on the safe use of digital technologies and online environments.

The procedure should also be reviewed and updated in response to any changes to the Safe use of digital technologies and online environments policy or following any incident or identification of risks relating the use of digital technologies and online environments.

Any revisions to the procedure should be communicated to staff and families, and access to electronic and hardcopies of older versions should be removed.

Duplicate (copy/paste) the below table to record each version change.

Version:	1
Approved by site leader:	Rowena McAvaney
Date of approval:	17/9/25
Date of next review:	16/9/28
Amendments(s):	New Procedure