Safe Use of Digital Technologies and Online Environment Policy inclusive of the E-safety policy

(Sourced: eSafety Early Years Online safety for under 5s: eSafety Checklist for Early Learning Services and Privacy Act 1988, ACECQA Policy and Procedure Guidelines Safe Use of Digital Technology and Online Environment Policy April 2026)
E-safety.gov.au eSafety Commissioner

Aboriginal and Torres Strait Islander e safety in first Nations language
Videos in other languages | First Nations | eSafety Commissioner

Keeping yourself safe online
Connecting safely | First Nations | eSafety Commissioner

Policy Statement

At **Snuggles**, we recognise the value that communication and digital technologies play in supporting the learning and development of young children. As part of our commitment to providing high-quality education and care, we offer children supervised access to Information and Communication Technology (ICT) equipment to help develop essential digital literacy skills for lifelong learning.

We also acknowledge the potential risks associated with the use of digital technologies and online environments. To ensure children's safety and wellbeing, we implement robust policies and procedures that protect children, educators, families, and visitors. This includes strict guidelines for the safe use, storage, and management of digital content, such as images and videos, and the secure use of digital devices.

All practices at Snuggles align with the **Statement of Regulatory Expectations (SRE) National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care**. We are committed to upholding children's rights to safety, privacy, and dignity while using digital technologies within our service environment.

Snuggles Early Learning Centre considers the safety, rights and best interests of children as the paramount consideration when developing policies and procedures.

Policy Background

This policy is intended to:

- Provide clear guidance and practical procedures to ensure that children are safe while accessing and using digital technologies and online environments as part of the educational program.
- Assist approved providers, nominated supervisors, and educators in meeting their **legislative obligations** to ensure every reasonable precaution is taken to protect children from harm and hazard, including those associated with digital technologies.

regulation 168(2)(h) – providing a child safe environment, including matters relating to the

- promotion of a culture of child safety and wellbeing within the service
  regulation 168(2)(ha) (which comes into force on 1 September 2025) – the safe use of digital technologies and online environments at the service, including:
  - the taking, use, storage and destruction of images and videos of children being educated and cared for by the service
  - obtaining authorisation from parents to take, use and store images and videos of children being educated and cared for by the service
  - the use of any optical surveillance device at the service including CCTV

- the use of any digital device issued by the service
- the use of digital devices by children being educated and cared for by the service.

regulation 168(2)(i) – staffing, including:

- a code of conduct for staff members
- determining the responsible person present at the service
- the participation of volunteers and students on practicum placements.

- Raise awareness among staff, parents/carers, and stakeholders about the potential risks associated with digital and online technologies, while also promoting their educational and developmental benefits.
- Define acceptable and responsible use of digital devices, storage, and content management by all individuals within the setting.
- Ensure that adults are aware of the correct procedures to follow in the event of any misuse of technology or breaches of policy.
- Establish safeguards and control measures for:
  - The taking, use, storage, and destruction of images and videos of children.
  - Obtaining written authorisation from parents/carers before any digital media of children is created or used.
  - The restricted use of optical surveillance devices (e.g. CCTV), ensuring transparency and regulatory compliance.(Refer to procedural documentation)
  - The exclusive use of service-issued digital devices to take or store images/videos of children.(Refer to procedural documentation)
  - The use of any digital device issued by the service.(Refer to procedural documentation register)
  - Strict and appropriate controls are in place for storage and retention of all digital content (images and recordings) involving children (National Model Code Part 4) (Refer to procedural documentation register)

Personal electronic devices that can take images or videos, and personal storage and file transfer media, are not to be in the possession of any person while providing education and care and working directly with children, unless for authorized essential purposes such as emergencies, health and family needs (National Model Code Part 2) and this use will only be authorised where access does not impede the active supervision of children.

This policy and principles and procedures aligned with the policy implementation, applies to all individuals involved with the service, including staff, educators, regular visitors, incursion staff and volunteers; children in our care; parents and carers; contractors, and committee members. It also applies to anyone using or bringing digital devices onto the premises, as well as individuals who are issued with service-issued devices for off-site, work-related use.

Legislative Requirements

The policy is consistent with, and refer to, the following legislative requirements.

Section/Regulation	Description
Section 2A	Paramount Considerations - safety, rights and best interest of children
Section 162A	Child protection training

Section 162B	Child Safety Training
Section 165	Offence to inadequately supervise children
Section 166	Offence to use inappropriate conduct
Section 166A	Offences relating to inappropriate conduct
Section 167	Offence relating to protection of children from harm and hazards
Sections 175A to 175J	Digital devices in education and care services
Regulation 84	Awareness of child protection law
Regulation 115	Premises designed to facilitate supervision
Regulation 122	Educators must be working directly with children to be included in ratios
Regulation 123	Educator to child ratios – center-based services
Regulation 128B	Child Protection training
Regulation 128D	Foundation child safety training
Regulation 128E	Advanced child safety training
Regulation 165	Record of visitors
Regulation 166	Children not to be alone with visitors
Regulation 168	Education and care services must have policies and procedures
Regulation **168 (2)(h)**	providing a child safe environment, including matters relating to the promotion of a culture of child safety and wellbeing within the service regulation 1**68(2)(ha)** (which comes into force on 1 September 2025) – the safe use of digital technologies and online environments at the service, including:
Regulation 168 (2) (i)	Staffing
Section 167	Offence relating to protection of children from harm and hazards
Regulation 170	Policies and procedures to be followed
Regulation 171	Policies and procedures to be kept available
Regulation 172	Notification of change to policies or procedures
Regulation 175	Prescribed information to be notified to Regulatory Authority
Regulation 176	Prescribed information to be notified to Regulatory Authority
Regulation 179A	Prescribed information to be kept in written record of authorisation to possess or control personal device
Regulation 179B	Prescribed period to keep written record of authorisation to possess or control personal device

Principles to inform Snuggles policy

At **Snuggles**, we are committed to ensuring children's health, safety, and wellbeing at all times, including when digital technologies and online environments are part of their learning and play. All decisions and practices relating to the use of digital devices are guided by the following principles:

- Children's health, safety, and wellbeing are paramount. We maintain a strong child safe culture that extends into digital spaces. All practices align with the Child Safe Standards, Mandatory Reporting obligations, and our broader Providing a Child Safe Environment Policy.
- Children are active participants in their digital experiences. We respect children's rights and agency and involve them, in developmentally appropriate ways, in decisions about using technology—including the taking, use, or sharing of their images or videos. We create supportive environments where children feel confident to ask questions, express discomfort, and disclose concerns without fear of reprisal.
- Active supervision is essential when children use digital technologies. Educators are expected to provide *intentional, vigilant, and continuous* supervision whenever a child is using a digital device, especially when accessing online content. Active supervision means more than just being in the same room—it includes actively engaging with the child's activity and being ready to intervene for instance: Identifying and responding to children who may be at risk of or are experiencing abuse or maltreatment through digital technologies and online environments This is vital to help prevent high-risk behaviours such as:
    - Uploading or sharing private information or images
    - Accessing inappropriate content (inadvertently or deliberately)
    - Making in-app purchases
    - Interacting with unsafe individuals
- Our educators, staff, and management are trained and responsible. All team members understand their roles in identifying and responding to risks of harm or abuse, including those that may arise through digital technologies. We ensure educators are trained in safe digital practices and are aware of how physical environment design (Regulation 115), supervision duties (Section 165), and educator ratios (Regulations 122–124) contribute to child safety.
- Families are respected partners in digital safety. We actively involve parents and carers in decisions about children's use of technology at the service. Parental authorisation is required before capturing, storing, or sharing any images or videos of children. We maintain open and transparent communication to ensure families feel confident in how digital technologies are used.
- Reasonable precautions and robust procedures are in place. We take all reasonable steps to prevent harm by ensuring appropriate supervision, restricting the use of personal devices, using only service-issued devices for capturing media, and following secure storage and destruction protocols. We have clear, rehearsed procedures for managing disclosures, incidents, or breaches related to digital safety.
- We adopt and implement the National Model Code. This ensures that all decisions about the use of digital and electronic devices across the service reflect child-safe principles and establish clear expectations for educators, staff, and volunteers.
    - Part 1: Only service-issued electronic devices should be used when taking images or videos of children while providing education and care.
    - Part 3: Essential purposes for which use and / or possession of a personal electronic device may be authorized for purposes other than taking images or recording videos of children include:

- communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises
- personal health requirements, e.g. heart or blood sugar level monitoring
- disability, e.g. where a personal electronic device is an essential means of communication for an educator or other staff member
- family necessity, e.g. a worker with an ill or dying family member
- technology failure, e.g. when a temporary outage of service-issued electronic devices has occurred
- local emergency event occurring, to receive emergency notifications through government warning systems, for example, bushfire evacuation text notification.

Key Terms

Term	Meaning	Source
Capturing, storing and transmitting images of children	Capturing an image includes filming, recording a video or taking a photo/image of a child. Storing means keeping the photo/image or video saved on a device, including a storage device. Transmitting includes sharing a photo or video by text message, email, uploading to any social media or information sharing platform or any other form of distributing an image or recording.	
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.	Glossary to NQF Child Safe Culture and Online Safety Guides
Cyberbullying	When someone uses the internet to be mean to a child or young person so they feel bad or upset.	
Disclosure	A process by which a child conveys or attempts to convey that they are being or have been sexually abused, or by which an adult conveys or attempts to convey that they were sexually abused as a child. This may take many forms, and might be verbal or non-verbal. Nonverbal disclosures using painting or drawing, gesticulating, or through behavioural changes, are more common among young children and children with cognitive or communication impairments. Children, in particular, may also seek to disclose sexual abuse through emotional or behavioural cues, such as heightened anxiety, withdrawal or aggression.	
Generative artificial intelligence (AI)	A branch of AI that develops generative models with the capability of learning to generate novel content such as images, text, and other media with similar properties as their training data.	
Harmful content	Harmful content includes: • sexually explicit material • false or misleading information • violence • extremism or terrorism • hateful or offensive material.	
Illegal content	Illegal content includes:	

	• images and videos of child sexual abuse • content that advocates terrorist acts • content that promotes, incites or instructs in crime or violence • footage of real violence, cruelty and criminal activity.	
Personal device	A personal device is a device that is owned by a person (NOT owned/supplied by an approved provider for education and care purposes) and is capable of capturing, storing or transmitting an image, for example phones, cameras, tablet computers, and hard drives.	Guide to the NQF (Glossary)
Service-authorised device	A service-authorised device is a device that has been authorised by an approved provider of a family day care service to be exclusively used for providing education and care, including to capture, store or transmit images of children. This device may not be owned by the approved provider or service. This may include devices such as phones, cameras, tablet computers, and hard drives. A service-authorised device must not be used for personal purposes.	Guide to the NQF (Glossary)
Service-supplied/issued device	A service-supplied device is a device that is owned or supplied by an approved provider to be exclusively used for providing education and care, including to capture, store or transmit images of children. This may include devices such as phones, cameras, tablet computers, and hard drives. A service-supplied/issued device must not be used for personal purposes.	Guide to the NQF (Glossary)
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender	
Sexting	Sending a sexual message or text, with or without a photo or video. It can be done using a phone service or any platform that allows people to connect via an online message or chat function.	
Smart toys	Smart toys generally require an internet connection to operate as the computing task is on a central server.	
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed. It can be with a stranger or someone you/the child knows.	

Procedures

Taking Images (SRE -National Model Code)

Using service-issued electronic devices appropriately

- **How does Snuggles document that an electronic device is issued for use at the service?**
  At Snuggles we maintain a register that outlines all digital equipment that is used and stored within our environment (Refer to procedural documentation (A))
  Equipment is purchased to support quality practice in the implementation of programming and planning and to further support communication with parents
- **What factors do you consider when planning for electronic devices to be accessible amongst your different rooms?**
  The factors that are considered when planning for electronic devices to be accessible for our rooms, is based on the age and the needs of the group, the needs of the educators to implement and embed best practice curriculum and communication techniques and the supports that are embedded to promote and maintain our community engagement within the environments in which the technology is used.

- **Do educators share electronic devices across rooms or have one per room? How are the images captured used for planning and programming?**
  The number and type of devices each room's community accesses is dependent on how the program and planning has been developed to support the interests, wellbeing, inclusive practices and the learning needs of the children. Educators may share devices depending on situational needs to implement, sustain and maintain engagement of their community. In most instances, the centre's programming and planning drives the taking of images/recordings on iPads. Images may often be used to support documentation of children's learning, (Using the theoretical philosophy of the center's Reggio Emilia approach - the One Hundred Languages) Images can promote and further the engagement of children in a the program, images may also further elaborate and readily document a visible example of educator concerns ie) of child engagement and interaction or images can be used to support procedural outcomes for each room i.e routines,
  Images of intentional and incidental teaching strategies can be used to capture play, visually capturing children making real contributions to the program through decision-making, where curiosity drives, and images record a learning journey.
  These images are all captured in the course of the learning journey within each room where educators are working with children and children have consented to the images being recorded.
- **Have you undertaken a risk assessment for usage of service-issued electronic devices, including during excursions or for transporting children?**
  Whilst the centre does not undertake excursion or the transportation of children, risk assessments continue to underpin processes to support the safe usage of digital technology within the center environment. As technological advances occur in this space we continue to remain diligent in our assessment of how to minimise digital risk to all members of our community.(Refer to procedural documentation inclusive of the Digital Register (B))
  Educator Supervision is a priority that is maintained at all times. No device may at any time be used to replace educator supervision at this service. Our adherence to ratio requirements and the distribution of educators through effective communication strategies supports implementation technology (images and recordings) within the service. Information recorded using devices is supported by our community where educators and children record together the child's learning journey and this technology helps to support children to be active members of the learning environment. The technology also supports effective and timely communication with our parents/guardians and the wider community.
  The service does not use Social Media platforms to share images or recordings of children.
- **How do you review the usage of the service-issued electronic devices currently? How often does this occur? Is there still a need for images and videos to be retained, or have they served their purpose?**
  Detailed in (Refer to procedural documentation (B) inclusive of the Digital Technology Parent Authorisation) at Snuggles we have an audited record of Digital technology involving the taking, using, storing and destruction of images and video recordings of children. This is reviewed by leading educators to ensure the timelines outlined for the usage, storage, retention and destruction are adhered to.(Refer to procedural documentation on the taking, use, storage, and destruction of images and videos of children (B) and the flow charts)
- **How do you support staff when using service-issued electronic devices to capture children's learning to also ensure adequate supervision of children?**

Snuggles purposefully has spent much time engaging with educators to support how, where and when information is captured, how it is stored, how it is used, and how it is disposed of. We are guided by our service Philosophy, the National Regulations with ratio, and the National Quality Standards for effective supervision, staffing arrangements and curriculum delivery, with the use of best practice standards.
Regular professional development underpins staff understandings of purposeful and meaningful delivery and documentation of curriculum initiatives and teamwork drives the effective implementation and inclusion of digital technology within the context of a tool for curriculum delivery, documentation and reflection.

How do you support educators to ensure child-centred image taking that is purposeful and supports quality educational practice and reflection, as well as family connection?
Our curriculum is supported by technological advances as opposed to driven by them. Our educators are highly trained and skilled as teachers and educators. Our philosophy, Mission and Vision statements are heavily focused on educator and child interactions and relationships, providing an environment for meaningful and purposeful learning and development, in which children thrive. We as a service take pride in the lack of technology used to drive curriculum initiatives. We have an embedded grass roots approach to capture and document learning in the moment, with the child, and share developments and progress with our community to support a home centre partnership, sharing and documenting each child's individual and collective learning journey. We use the advancements in technology as an effective tool to support this connection, communication and documentation, by providing a visual representation of learning in action. Snuggles does not use Social Media platforms to share images or recordings of children but rather creates home center partnerships and connections to establish, facilitate, maintain and sustain two way meaningful family connection and communication.

How do you monitor who is using service-issued devices to take images or videos of children?
All educators are considered to be responsible to action program delivery which support child's learning and development and as such they require access to devices and materials to support them to fulfil their role to the best quality standards.
Agency staff and Students who are not members of the Snuggles staffing community are prohibited from using the Snuggles digital technology or personal devices whilst in the care and education of children. Snuggles educators will enforce this policy.

- **When is it appropriate to take images or videos of children using a service-issued electronic device? Have you considered other circumstances where you may be asked to take images or videos that are not for recording a child's learning, for example, to record an injury or if asked/instructed to take an image of a child by the Police or a Child Protection Agency?**

  Whilst limited in necessity, there may be circumstances that require/ask or instruct Snuggles staff to record an injury or to take an image of a child ie) by the Police or a Child Protection Agency or a recognised authority (ISE). In this instance, if required we would seek further clarification of the requirement with the regulator (ACECQA, VECRA) and make a centre based informed decision based on the request. Snuggles staff would use the CISS and

FVISS Decision Tree to help support their decision and record and have witnessed this action, with the responsible person in charge of the centre and where possible, either the nominated supervisor and/or Approved provider. (Refer Authorised Image/Video Sharing Record)

- Approved providers **cannot ever** authorise the use of a **personal device** to take images or videos of children.

- **How will you manage families, external visitors, or organisations engaged by the service and their taking images or videos of children, for example, photo day or marketing or external activities / presenters, or excursions where the presenter would like to take photos for their own purposes?**
  We have a No Personal Devices initiative in all rooms where there are children in the care and education at Snuggles. This is represented visually and communicated through policy development and implementation and event management emails to all of our community. This means that we request families, external visitors, and/or organisations engaged by the service to refrain from taking images or videos of children. We request that personal devices and smart watches are not worn or taken into the rooms by staff, regular visitors, and allied health support staff.
  Allied health staff are requested to limit the use of organisational issued IT for the purpose of their visit however personal devices are prohibited
  We request and enforce that families do not use personal devices to record images or videos, inclusive of but not limited to, phones, smart watches, video recording technology and cameras, whilst in the rooms with children.

- **If a student as part of their practicum wants to take images of children, do your service's policies and procedures permit this via appropriate use of a service-approved devices?**
  Students are prohibited from taking images/recordings of children whilst on placement. Students whilst supervised by their mentor educator(s) may use the service issued ipad to take an image of a work sample which does not include children, for the purpose of their assessment.

- **Have you conducted a risk assessment to ensure an adequate number of telecommunications devices are still readily available at all times for essential communications, including in the event of a serious incident or emergency? Specific attention should be paid to when services are on excursions and other scenarios outside the service premises.**

  Snuggles supports an integrated telecommunication/intercom system that readily connects with all rooms,and external services to the service. (4 rooms plus staffroom kitchen, office and reception included) Staff are rostered to ensure communications in an emergency can effectively support proactive communications.

  A cellular emergency ipad enables the centre to contact parents from an off site location should an off site emergency evacuation occur or should there be a situation where the telephone system is down.

Creating a child safe culture

- **How do you support all staff to maintain / create a culture of child safety and to speak up if they see personal electronic devices being used, or service-issued electronic devices being used inappropriately?**

  Staff are empowered through a clear organisational structure and training plan inclusive of Mandatory Reporting, our annually reviewed Emergency Management Plans, the Providing a Child Safe Environment Policies and Procedures, the Reportable conduct scheme, and this policy's breach procedures to report misconduct of any nature to both their Leading Teacher and Management.

  Any misconduct will be investigated and action/reporting will be determined based on, but not limited to, the guidelines of the Snuggles Policies and Breach Procedures, the Reportable Conduct Scheme, The Child Safe Standards and the National Regulation requirements.

  The staff at Snuggles sign a contract which contains a statement of commitment to uphold the 11 Child safe standards, the staff code of conduct and the code of Ethics, they complete annual Mandatory Reporting and Child Safe Training which regularly asks staff to reflect on practices that support the provision of a safe learning environment.

- **What parts of your service should be off limits for taking or recording images or videos of children? e.g. in bathrooms and nappy change facilities, cot rooms, a cubby or places where another educator or other staff member cannot see the image being**

  Images or videos of children are limited to shared play spaces and only taken where the purpose is clear and acceptable to all educators engaged in the room program. Educators need to be purposeful in their documentation of learning and responsible to ensure the safety of all children including when images and recordings are conducted.

- **How do you gain consent to having a child's image taken or recorded while providing early childhood education and care?**

  Consent from families regarding images and recordings is explained and gained upon enrolment. It is the responsibility of the parent/guardian to notify the service in writing if permissions are withdrawn.(Refer Digital Technology Parent Authorisation template)

  Consent of the child is always sought to uphold their right to make decisions around how and when they would like their learning recorded.

- **What controls, settings or restrictions on service-issued electronic devices have in place that can minimise the risk of them being used inappropriately ?**

  Staff rostering is monitored to effectively embed the Child Safe Standards in practice, protecting children from harm and hazard, and as such effective supervision, communication, implementation and reflection on the program, inclusive of the room operations and staffing expectations, aims to embed practice and reduce the risks posed by the usage of service-issued electronic devices.

- **Have you considered alternatives to when staff may have been using their personal electronic device to undertake work-related activities, such as excursions for keeping**

in contact with the service or checking the UV rating at the service through an app to determine if outdoor play and/or its length is appropriate?

We do not undertake excursions however staffing arrangements ensure effective centre communication in the event of an emergency.

The Apple Ipads have an embedded application for UV ratings for staff to access.

No image/recording of children who attend the centre can be stored anywhere but on service issued devices All work related activities containing images and/or recordings of Snuggles children may only be undertaken on the service issued devices.

- **How will you manage special events at your service where families may attend and want to take images or videos of children?**

  The use of personal devices that can take and record images/videos are prohibited at Snuggles whilst children are being cared for and educated at the service. As such, this applies to the use of personal devices by all members of the community. As we respect a families desire to capture memories of special occasions, we provide extra staffing at events to support the taking of images/videos to be shared on family approved platforms as outlined in our parent authorisations.

- **How do you communicate with families about when and how you will take and use images and videos of their child/ren and formally seek their agreement to this? Do you have appropriate parent / guardian permissions to take and share images and video recordings of children for clearly stated purposes?**

  On enrolment image and video recordings form part of the permissions. This is also a conversation that we hold with families to clearly explain the purpose and the publications in which their child's photo or a recording of their child may appear. (Refer Digital Technology Parent Authorisation template)

- **How do you manage personal devices that children with additional needs may require access to within your service?**

  Individual requirements are assessed and action plans developed on an individual needs basis (with the support of allied health professionals, Inclusion support officers PSFO, KESO's, or other support services where required) to support the inclusion of all children to the service. If this includes the use of personal devices, risk assessments will be undertaken with the input of families and their support staff, to support Snuggles educators to mitigate any potential risks identified.

- **How do you provide advice to educators about which images to share on social media, such as through apps for communicating with families?**

  Snuggles is purposeful in its decision not to engage in social media platforms for the regular sharing of images and communication with families.

- **How do you gain authorisation / consent in relation to other professionals that are not engaged by, but are supporting children at the service (e.g. NDIS funded support**

professionals, Inclusion Support professionals), and who may have a legitimate need to capture an image or video of a child?

Allied health or support professionals that visit the service are requested to limit the use of organisational issued IT for the purpose of their visit. Personal devices are prohibited. Families of children who request allied health to support their child whilst at the service will be provided with a letter that outlines the use of digital technology at the service and requested to ensure that their service provider is aware of the Snuggles procedure before attending the service. (Refer: Code of Conduct for Regular Visitors – Digital Technology Procedure)

Use of personal electronic devices

- **How do educators, other staff and volunteers make or receive personal phone calls / communications when required at your service?**

  Personal devices are prohibited for use in the care and education of children However there are some exemptions to this provision.

  Exceptions to the restrictions regarding personal devices

  Where use and/or possession of a personal electronic device may be authorised include:

  - emergency communication during excursions, transportation of children and regular outings (for example, for when groups of children and educators get split up)
  - emergency communication when children are transported or travel on transport arranged by the service
  - communication in an emergency situation involving a lost child, injury to child or staff member, or other serious incident, or in the case of a lockdown or evacuation of the service premises
  - personal health requirements (for example, heart or blood sugar level monitoring)
  - disability (for example, where a personal electronic device is an essential means of communication for an educator or other staff member)
  - family necessity (for example, a worker with an ill family member)
  - technology failure (for example, when a temporary outage of service-issued electronic devices has occurred)
  - a local emergency event occurring, to receive emergency notifications through government warning systems (for example, bushfire evacuation text notification).

  In any of the above circumstances for exception, staff will be required to complete a log registering this use (refer Exceptions register - Use and/or possession of personal electronic devices)

- **Do you have secure storage for staff and volunteers to leave their phone and other personal belongings, such as a staff room with lockers? How do you ensure educators can access their personal devices during times when they are not working directly with children, such as their breaks?**

Staff are required to leave all personal devices in their lockers and switch them to do not disturb mode whilst they are stored.

- **If staff are issued an electronic device for work purposes and also allowed to use it for personal usage, how do you ensure the safety of images and videos of children?**

  Where staff are permitted to use service-issued electronic devices for limited personal purposes, the safety and confidentiality of images and videos of children remain a top priority.Staff are to follow the Snuggles procedures and policies in place for the storage, sharing and destruction of images/videos. Passwords further protects images and video accessibility on devices and cyber security protections ie) Norton are in place to support overall safety of the technological environment.

  All images and videos of children must be **stored securely** on approved systems and never shared or backed up to personal devices/accounts or external cloud storage.

  Personal use must never interfere with the protection, privacy, or management of children's information.

  Devices are subject to **routine monitoring**, and staff receive ongoing guidance to ensure safe and appropriate use.

- **How do you allow staff / educators to apply for an exception to access a personal electronic device as an essential reason, such as where medical reasons require a device to be on them at all times? How do you document these arrangements?**

  Individual requirements are assessed and action plans developed on an individual needs basis (and with external support services input where required) to support the inclusion of all educators within the service. If a staff member requires the use of personal devices for an essential reason, a risk assessment will be undertaken with the input of management and actions recorded within the Exceptions register - Use and/or possession of personal electronic devices, to support all staff to be aware of and mitigate any potential risks identified.

- **How will you ensure visitors and families to the service are aware of your policy for educators and other staff, and if you have one specifically for families in relation to not taking images or videos of children?**

  This policy will be shared with all families 14 days prior to publication.

  As we continue to support best practice and as this is an evolving issue with the need for input from all areas of our community, parents will be invited to read, discuss and contribute thoughts to this policy in a round table forum with educators. This conversation will be ongoing as implementation may highlight further need to improve this documentation.

Planning and Programming

Images used in emails, Newsletters and program documentation may be temporarily stored on service issued computers whilst compiling data for educational purposes. No images are to be shared beyond the Snuggles community.

It is the expectation of Snuggles Management and staff that all content and images/videos that are shared via email/dropbox with families of enrolled Snuggles children, remain within our community, and as such this respects the privacy of each enrolled member of the Snuggles community.

Any uploaded videos and resources developed by staff remain the property of Snuggles Early Learning Centre.

Digital Technology with Children referencing the National Model Code

Digital technology (e.g., iPads) may be used occasionally and purposefully to support children's engagement in learning, i.e. movement-based and sensory experiences, such as:

- Yoga and music sessions that are short and actively facilitated by an educator;
- Activities that promote physical activity, coordination, and connection through singing, stretching, reaching, or gentle movement;
- Programs or videos selected to support early development goals — always age-appropriate, non-commercial, and free from advertising.

Safe and Supported Practices

- Children will never be left alone with digital devices. (including smart toys)
- These digital activities are used sparingly.
- Screen-based activities do not replace physical play, tummy time, or interpersonal interactions.
- Digital tools are used in a way that promotes active participation, not passive viewing.
- Wallpaper for each of the centre issued devices is readily recognisable for educators and older children
- Through open communication, joint decision making practices and child advocacy, children are actively engaged in learning about how to report concerns or feelings of being 'unsafe' in an online environment - this is a natural progression from teaching and developing the physical safety concepts taught within their familiar context and transferring their knowledge of safety to an online learning environment. Concepts of privacy and consent will be explored through this lens to support child learning and development.

Commitment to Developmentally Appropriate Use

- We ensure that any use of technology aligns with current early childhood development research and health guidelines.
- Our educators are trained to assess when and how digital technology can be used in a way that is safe, meaningful, and supportive of a child's overall development.
- Children are taught during the usage of technology safe use strategies to support their learning and development in a digital world.
- Safe use practices are role modeled to children during these interactions.

Personal Phone numbers

- Staff are advised not to share personal information with families at the service.

Personal Email addresses

- Staff are assigned Snuggles emails for all work related activities.

WeChat Staff forum

- Only members of the current staffing community form part of the Snuggles WeChat group
- No photos are to be shared of Snuggles enrolled children in this forum.
- No staff should at any time feel pressured to comment on this page.
- Any staff not willing to be a member of this group may choose to leave the group at any time without explanation.
- The WeChat staff forum can be accessed during operational hours to deliver work related messages but may not be accessed for any reason when working directly with children at the service. .
- Outside of hour communications do not require staff to respond

Internet

- Our internet server is protected by Norton.
- Our expectation is that staff will only use IT service issued devices provided by the centre for educational purposes.

Reporting Cyber-abuse

Should an educator believe that they are subjected to cyber-bullying, the educator should follow the following steps.

Step 1 Collect evidence and information.
Take a screenshot from your device. Write down the evidence and information.
Step 2 Report to the social media service or platform where the cyber abuse took place.
Refer to the e-Safety Guide (https://www.esafety.gov.au/key-issues/esafety-guide) for the reporting links of social media services, apps, games and websites.
Step 3 Make an adult cyber abuse report to e-Safety.

Connecting with Families

- Information on appropriate online safety and e-safety policies are communicated to families through our newsletters, displays and emails.
- Multiple educators at Snuggles speak a variety of languages and can assist parents in the understanding of the information and policies.
- Parents are made aware that they can go to Snuggles Management and the e-Safety Commissioner for help with online safety issues.

Reporting a Breach of the Policy

- For detailed Breach Reporting please refer to
    - Cyber Security Breach Procedure
    - Staff Member/Student and Volunteer Breach of Procedure
    - Parent/Guardian Breach Procedure

Links to other policies

This policy if related to the following policies:

- Providing a Child Safe Environment Policy
- Incident, injury, trauma and illness Policy
- Dealing with Complaints Policy
- Acceptance and Refusal of Authorisations Policy
- Staffing Employment and Recruitment Policy
- The Staff Handbook, Induction, Staff Code of Conduct and Statement of Commitment to Child Safety
- The Code of Conduct for Regular Visitors
- The Cyber Security breach procedure
- The Student Teacher Handbook and Induction
- The Parent General Information, The Enrolment Handbook and The Digital Technology Policy Authorisation
- The Breach of Snuggles Use of Digital Technologies and Online Environments policy/log
- Governance and Management Policy
- CCTV policy and procedures
- Child Mental Health and Wellbeing Policy
- Excursion and Incursions Policy
- Inclusions Of Children with Additional Needs
- Interaction with Children Policy
- Supervision Policy
- Safe Transportation of Children Policy

Induction and Ongoing Training

Implementation of the policy will be monitored by management on an on-going basis and it will be reviewed annually by the trustees unless an incident occurs in which this will trigger a thorough review of the policy and procedures.

Resources and Support

Related documents

- eSafety Checklist for Early Learning Services
- eSafety Early Years program for educators
  https://www.esafety.gov.au/educators/esafety-early-years-program-for-educators

- Aboriginal and Torres Strait Islander e safety in first Nations language
  Videos in other languages | First Nations | eSafety Commissioner

- Keeping yourself safe online
  Connecting safely | First Nations | eSafety Commissioner

- Child safe practices for digital technologies and personal electronic devices | vic.gov.au

- ACECQA National Model Code https://www.acecqa.gov.au/national-model-code-taking-images-early-childhood-education-and-care

- VECRA Personal device restrictions in early childhood education and care services https://app.vision6.com.au/v/106088/1249557/email.html?k=DsHq8Vmg2GPxqau_biQ37I0-BFM0uUAbX5kXv8CQnnc
- NATIONAL MODEL CODE FOR EARLY CHILDHOOD EDUCATION AND CARE
- Education and Care Services National Regulations (2011 SI 653) - NSW Legislation
- Centre-based services: child safety and personal electronic devices https://www.vic.gov.au/centre-based-services-child-safety-and-personal-electronic-devices

Policy Created/Reviewed

This review will be done in accordance with regulations.

Policy reviewed	**May 2026**
Policy Review Date:	**September 2027**