Safe Use of Digital Technologies and Online Environments

Policy Title	Safe Use of Digital Technologies and Online Environments
Policy version	V2
Review Cycle	2 Years
Last Review Date	October 2025
Implementation Date	February 2026
Next Review Date	February 2028

Policy Statement

SHARE OOSH is committed to protecting children's safety, wellbeing, dignity and privacy in all physical and online environments. In accordance with Regulation 168(2)(ha) of the Education and Care Services National Regulations and the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 (NSW), the service maintains clear systems to ensure the safe, lawful and professional use of digital technologies and online environments.

Our Service adopts and aligns with the National Model Code for taking images or videos of children.

Definitions

Artificial Intelligence (AI)	An engineered system capable of generating content, predictions, recommendations or decisions based on defined inputs or objectives without explicit task-specific programming.
Digital technologies	Service-issued electronic devices and associated applications or software used within the service for program or administrative purposes.
Harmful content	Harmful content includes sexually explicit material; false or misleading information; violence; extremism or terrorism; hateful or offensive material
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
Online environments	Internet-based platforms or digital spaces accessed by the service, educators or children, including streaming services, communication platforms and approved applications.
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender
Personal devices	Any mobile phone, smart watch, tablet, wearable device, camera or similar device that is not owned or managed by the service and is capable of capturing, storing or transmitting images, audio or data.
Service-owned devices	An electronic device purchased, supplied and managed by the service for authorised program or administrative use.
Social media	Platforms that enable sharing of information, images or videos online (e.g. Facebook, Instagram, TikTok, WhatsApp).

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2	Safety	Each child is protected.
2.2.1	Supervision	At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.
2.2.3	Child Safety and Protection	Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk, including risks that may arise from digital environments.

QUALITY AREA 4: STAFFING ARRANGEMENTS		
4.2.2	Professional standards	Professional standards guide practice, interactions and relationships, including expectations for responsible use of technology.

QUALITY AREA 7: GOVERNANCE AND LEADERSHIP		
7.1.2	Management systems	Systems are in place to manage risk and enable the effective management and operation of a quality service that is child safe.

EDUCATION AND CARE SERVICES NATIONAL LAW	
162A	Child protection training
165	Offence to inadequately supervise children
166A	Offence to subject child to inappropriate conduct

167	Offence relating to protection of children from harm and hazards
EDUCATION AND CARE SERVICES NATIONAL REGULATIONS	
12	Meaning of serious incident
73	Educational Program
76	Information about educational program to be given to parents
84	Awareness of child protection law
115	Premises designed to facilitate supervision
122	Educators must be working directly with children to be included in ratios
123	Educator to child ratios – centre-based services
149	Volunteers and students
155	Interactions with children
156	Relationships in groups
160	Child enrolment records to be kept by approved provider and family day care educator
162	Health information to be kept in enrolment record
168	Education and care service must have policies and procedures
168(2)(ha)	Policies and procedures for the safe use of digital technologies and online environments
170	Policies and Procedures to be followed
171	Policies and procedures to be kept available

172	Notification of change to policies or procedures
175	Prescribed information to be notified to Regulatory Authority
176	Time to notify certain information to Regulatory Authority
181	Confidentiality of records kept by the approved provider
182	Storage of records and other documents
183	Period of time records are to be kept
184	Storage of records after service approval transferred

Related Policies

- Providing a Child Safe Environment
- Interactions with Children
- Supervision
- Behaviour Guidance
- Confidentiality
- Child Safe Code of Conduct
- Enrolment and Orientation
- Excursions and Regular Outings

Purpose

The purpose of this policy is to establish clear and consistent expectations for the safe use of digital technologies and online environments at SHARE OOSH. The policy supports the service to meet its obligations under the Education and Care Services National Law and Regulations, including Regulation 168(2)(ha), and applicable NSW Ministerial Orders relating to electronic devices.

This policy aims to:

- Protect children from harm, exploitation, inappropriate content, and misuse of digital technologies.
- Safeguard children's privacy and personal information.
- Ensure personal electronic devices do not compromise supervision, professional conduct, or child safety.
- Provide guidance on the secure use, management and storage of service-issued devices.

- Support responsible and limited use of digital technologies within the educational program.

- Establish clear processes for responding to digital risks, incidents, and breaches.

Scope

This policy applies to children, families, staff, educators, management, approved provider, nominated supervisor, students, volunteers and visitors of the OSHC Service.

Guiding Principles

SHARE OOSH is guided by the following principles in relation to digital technologies and online environments:

1. **Child safe culture extends to digital environments** – The service maintains a child safe culture in both physical and online settings, recognising that risks to children may arise through digital technologies.

2. **Children's wellbeing and rights are paramount** – Children's safety, dignity and privacy are prioritised in all decisions relating to digital technologies, including decisions about images, recordings and online access.

3. **Shared responsibility and active supervision** – Approved Providers, Nominated Supervisors, Responsible Persons, educators, staff, volunteers and students understand their roles in preventing, identifying and responding to digital risks and exercise reasonable precautions and active supervision at all times.

4. **Clear expectations and lawful practice** – The service adopts the National Model Code and applicable regulatory requirements to establish clear expectations for the safe, professional and lawful use of electronic devices.

Procedures

To uphold this policy, SHARE OOSH will implement the following procedures:

1. Personal Electronic Devices

To uphold child safety and comply with the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 (NSW), personal electronic devices must not be in the possession of educators, staff, volunteers or students while working directly with children.

For the purpose of this policy, personal electronic devices include mobile phones, smart watches, tablets, wearable devices, cameras and any device capable of capturing, storing or transmitting images, audio or data.

The restriction applies during:

- Indoor and outdoor program time

- Excursions and regular outings

- Transportation of children

- Any period in which the individual is counted in educator-to-child ratios

Personal electronic devices must not be used to take photographs, record audio, access social media, send messages or conduct personal communication while working directly with children.

Personal electronic devices must be stored in the staff room or administrative office during shift hours and must not be accessible within program spaces.

If an educator or staff member steps into ratio or undertakes direct supervision responsibilities, they must ensure their personal electronic device is not in their possession prior to commencing those duties.

Personal electronic devices are not to be brought on excursions unless authorised under a prescribed circumstance in accordance with this policy.

Prescribed Circumstances
Where permitted under the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 (NSW), a prescribed circumstance authorisation may be granted by the Approved Provider.

Any authorisation must:

- Be documented in writing
- Specify the prescribed circumstance and duration
- Outline any conditions attached to the authorisation
- Be reviewed at least every three months
- Be retained for a minimum period of three years
- Be formally revoked in writing where applicable

Authorisations will only be granted where the criteria set out in the NSW Device Order are met.

Failure to comply with this section may constitute a breach of the service's Code of Conduct and may result in disciplinary action.

2. Service-Issued Devices

Only electronic devices supplied, issued and registered by SHARE OOSH may be used for operational, administrative or program purposes.

Service-issued devices include, but are not limited to, mobile phones, tablets, laptops or any electronic device capable of capturing, storing or transmitting images, audio or data.

Device Register
The service will maintain an Electronic Device Register for all service-issued devices. The register will include:

- Device type

- Make and model
- Serial number or unique identifier
- Date of purchase or issue
- Assigned user (if applicable)
- Confirmation that the device is configured in accordance with this policy

Devices will be clearly identifiable as service property where practicable.

Where a device is no longer in use, a record of revocation will be documented in the register.

Records relating to the supply, issue or revocation of service-issued devices will be retained securely for a minimum period of three years.

Camera Restrictions
Service-issued tablets (including iPads) are not to be used to take photographs or recordings under any circumstances. Camera features on tablets must remain disabled.

Where photographs are required for medical documentation purposes, only the Responsible Person service-issued mobile phone may be used in accordance with Section 4 of this policy.

Configuration and Security
All service-issued devices must:

- Be password protected
- Restrict unauthorised access
- Be used only for authorised purposes

Service-issued devices are configured with security settings, password protection and application restrictions to ensure only authorised applications and functions are available. The Service will implement a periodic review of service-issued devices to ensure security settings remain active and only authorised applications and data are present.

Service-issued devices may be shared between authorised staff. Staff must log out of systems after use and must not store passwords or personal login information on shared devices. Devices must not be used to access personal social media accounts or personal communications.

Images or service data must not be transferred to personal devices or unauthorised platforms.

Storage
Service-issued devices must be stored securely when not in use, in a manner that prevents unauthorised access or misuse. Service-issued devices are stored securely when the service is closed and are kept in a locked office.

Where devices are used during excursions or transportation, they must be securely managed and accessible only to authorised staff.

Service-issued devices are configured and managed by the Nominated Supervisor or Approved Provider. Security settings, passwords and application permissions may only be changed with their authorisation

3. Use of Digital Technologies with Children

Digital technologies may be used with children only where their use is purposeful, planned and consistent with the educational program.

Devices may be used to support learning, creativity, research, communication or structured group activities, provided that use aligns with the service philosophy and child safe practices.

Supervision and Visibility
When digital technologies are used with children:

- An educator must be actively supervising at all times.
- Devices must be used in open and visible areas of the service.
- Screens must remain visible to educators.
- Children must not be left unattended while using a device connected to the internet.

Content and Access
Educators must ensure that:

- Digital content accessed or viewed is age-appropriate, suitable for the developmental stage of the group, and consistent with community standards.
- Content depicting explicit violence, sexual material or themes inappropriate for primary-aged children is not shown.
- Children are supported to understand safe and respectful online behaviour.

Screen Time
Digital technology use must be limited and purposeful. Screen time is not to be used as a reward, behaviour management strategy or substitute for supervision.

Where digital media is used for entertainment purposes, educators must consider Australia's Physical Activity and Sedentary Behaviour Guidelines and ensure children continue to engage in active, social and play-based experiences.

App and Streaming Approval
Applications, streaming platforms and digital content accessed by children must be approved by the Nominated Supervisor prior to use at the service.

Educators must not independently download applications or install software on service-issued devices without prior approval.

When selecting streaming content (including platforms such as Netflix or Spotify), educators must ensure content is age-appropriate, consistent with community standards and suitable for the youngest child present.

Where reasonably practicable, devices will be configured to restrict unauthorised downloads and in-app purchases.

Risk Awareness
Educators must remain alert to digital risks, including:

- Exposure to harmful or illegal content
- Unwanted online contact
- Inappropriate searches
- Sharing of personal information

Any concerns arising during the use of digital technologies must be immediately reported to the Nominated Supervisor and documented in accordance with service procedures.

Children's Personal Electronic Devices
Children may bring personal electronic devices, including mobile phones, tablets, computers, smart watches, or smart toys to the service. However, personal devices must not be used at any time during attendance at SHARE OOSH.

Children's personal devices must not be used to:

- Take photographs or record audio or video
- Access the internet or social media
- Communicate with others during program time

Devices must remain stored in the child's bag or in a designated storage area for the duration of their attendance.

If a child uses a personal device in breach of this policy, the device may be temporarily removed and returned to the family at collection time.

The service is not responsible for the loss, damage or theft of children's personal electronic devices.

4. Images and Recordings

The service prohibits the taking of photographs, video recordings or audio recordings of children while they are being educated and cared for at SHARE OOSH, except as expressly authorised below.

This prohibition applies to:

- Personal electronic devices
- Service-issued tablets (including iPads)
- Service-issued laptops
- Any other device capable of capturing images, video or audio

A photograph of a child may only be taken where authorised by the Nominated Supervisor or Responsible Person for one of the following purposes:

- Documenting a significant injury
- Attaching to a medical management plan or medical risk assessment
- Inclusion in a child's medical bag or emergency medical documentation

Photographs must:

- Be taken only on the designated service-issued mobile phone
- Be directly related to the authorised purpose
- Be uploaded to the child's secure record as soon as practicable
- Be permanently deleted from the device immediately after upload, including from any "recently deleted" folders

Photographs must not be transferred to personal devices, used for promotional purposes, shared on social media or distributed outside authorised documentation systems.

All photographs taken under this section form part of the child's confidential record and are stored in accordance with Regulations 181–183 and the service's Privacy and Confidentiality Policy.

Families of children with diagnosed medical conditions are strongly encouraged to provide an updated headshot photograph where the existing image is no longer current. If an updated photograph is not provided and safe identification requires it, the service may take a current headshot in accordance with the authorised procedures above to uphold child safety.

5. Artificial Intelligence (AI)

Artificial Intelligence (AI) tools may be used for administrative or professional purposes, including drafting documentation or supporting planning processes.

When using AI tools, staff must:

- Not enter identifying information about children, families or staff
- Not upload confidential documents or records
- Review and verify all outputs for accuracy, appropriateness and professional judgement
- Ensure content aligns with the service philosophy, child safe practices and legislative requirements

AI tools must not replace professional decision-making, supervision responsibilities or child protection obligations.

Any use of AI must comply with privacy legislation and the service's Confidentiality and Records Management requirements.

6. Online Safety, Risk and Reporting

The service recognises that harm to children may occur through digital technologies and online environments. This includes exposure to inappropriate content, online bullying, unwanted contact, image misuse, or the sharing of personal information.

Educators and staff must remain vigilant to digital risks and actively supervise children when digital technologies are in use.

Identification and Immediate Response
If a child:

- Discloses online abuse or harm
- Is exposed to inappropriate digital content
- Engages in unsafe online behaviour
- Is the subject of image misuse or online bullying

Educators must:

- Immediately ensure the child's safety
- Preserve any relevant evidence where appropriate
- Report the matter to the Nominated Supervisor without delay
- Document the incident in accordance with service procedures

Reporting Obligations
Where online harm may constitute child abuse, reportable conduct, or a risk of significant harm, mandatory reporting obligations apply.

Where appropriate, matters may be reported to:

- The NSW Child Protection Helpline
- The eSafety Commissioner
- NSW Police

If an incident meets the definition of a serious incident under the National Regulations, the Regulatory Authority will be notified within 24 hours via NQAITS.

All incidents involving digital or online harm will be reviewed by the service to identify contributing factors and implement preventative measures.

7. Privacy, Data Protection and Breach Management

The service is committed to protecting the confidentiality, integrity and security of all child and family information in accordance with Regulations 181–183, the Privacy Act 1988 and the Australian Privacy Principles.

All digital records relating to children, families and staff must be:

- Accessed only by authorised persons
- Used solely for legitimate service purposes
- Stored securely within approved systems
- Protected by password access and reasonable security safeguards

Confidential information must be handled in a way that protects the privacy and safety of children, families and staff.

Operational communication about children may occur via phone calls, text messages or email where necessary for the safety, supervision or coordination of the service.

Personal devices must not be used to take, store, transmit or share photographs or videos of children. Images or video of children may only be captured using authorised service-issued devices and in accordance with this policy.

Staff must not screenshot, download or otherwise capture images or videos of children from service systems onto personal devices.

Service systems such as OWNA may be accessed on personal devices for administrative purposes (for example payroll, rostering or staff communications, meeting reporting timeframes) when staff are not working directly with children.

Access to digital records containing information about children, families or staff is restricted to authorised personnel and managed through role-based permissions within approved service systems. Access to sensitive records (such as staff files or child protection documentation) is limited to authorised management personnel.

Lost or Compromised Devices
Any loss, theft, unauthorised access or suspected compromise of a service-issued device must be reported immediately to the Nominated Supervisor.

The service will:

- Assess the risk to affected individuals
- Secure or disable the device where possible
- Determine whether an eligible data breach has occurred

Notifiable Data Breaches
Where a data breach is likely to result in serious harm to individuals, the service will comply with the Notifiable Data Breaches scheme, including:

- Notifying affected individuals
- Notifying the Office of the Australian Information Commissioner (OAIC)
- Implementing remedial actions to reduce risk

All data breaches or suspected breaches will be documented and reviewed to identify preventative improvements.

Device Disposal and Decommissioning

Service-issued devices that are damaged, replaced or no longer in use must be securely erased prior to disposal, transfer or recycling.

Secure erasure includes:

- Removal of all accounts
- Deletion of stored data
- Resetting the device to factory settings

Where reasonably practicable, confirmation of erasure and disposal will be documented in the Electronic Device Register.

8. Risk Assessment and Review

The service will maintain a written Digital Technologies and Online Environments Risk Assessment.

The risk assessment will identify and evaluate risks associated with:

- The use of digital technologies by children
- Service-issued devices
- Online environments accessed at the service
- Storage and protection of digital records
- Image capture for authorised medical purposes
- Emerging technologies, including Artificial Intelligence

The risk assessment will:

- Be reviewed at least annually
- Be reviewed following any digital or online-related incident
- Be updated where legislative or regulatory requirements change
- Inform staff training and procedural improvements

The Nominated Supervisor will be responsible for ensuring the risk assessment is completed, reviewed and implemented.

This policy will be reviewed:

- At least annually
- Following any serious incident involving digital technologies
- Where changes occur to legislation, regulations or NSW Orders

- Where operational practices change

Roles and Responsibilities

ROLE	RESPONSIBLE FOR
Approved Provider	• Ensure compliance with the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 (NSW), National Law and Regulations • Ensure this policy is implemented and reviewed • Authorise prescribed circumstance exemptions where applicable • Ensure an Electronic Device Register is maintained • Ensure adequate resources are provided to implement this policy
Nominated Supervisor	• Implement and monitor this policy in daily practice • Authorise any permitted medical photographs • Ensure service-issued devices are configured and managed in accordance with this policy • Ensure digital risk assessments are completed and reviewed • Respond to and document any online safety or data breach incidents
Responsible Persons	• Ensure compliance with this policy during their shift • Authorise permitted medical photographs where delegated • Monitor supervision of digital technology use • Report any breaches, lost devices or online safety concerns to the Nominated Supervisor
Educators	• Comply with restrictions on personal electronic devices • Use digital technologies only in accordance with this policy • Actively supervise children when digital devices are in use • Report any online safety concerns, incidents or suspected data breaches immediately • Protect the confidentiality of all digital records
Families	• Adhere to the Safe Use of Digital Technologies and Online Environments Policy and associated procedure • Not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the OSHC Service • Provide accurate enrolment information, including identification photographs • Provide updated photographs for children with medical conditions where requested • Raise any concerns regarding digital safety or information security with the service

Other Staff	• Comply with personal device restrictions when working directly with children • Maintain confidentiality of digital information • Report any concerns related to child safety, including inappropriate use of digital technology, to the Nominated Supervisor or Approved Provider
Students/Volunteers	• Comply with personal device restrictions at all times while working directly with children • Use digital technologies only under supervision and in accordance with this policy • Report any concerns to a supervising educator or Responsible Person

Induction and Ongoing Training

All educators, staff, students and volunteers will be informed of this policy during induction.

Induction will include:

- Overview of personal electronic device restrictions
- Expectations regarding service-issued device use
- Prohibition on photography except as authorised
- Online safety and reporting obligations
- Confidentiality and data protection requirements

Staff will be required to acknowledge their understanding of this policy as part of their induction process.

Ongoing training will include:

- Updates to legislative or regulatory requirements
- Refresher guidance on digital risk and online safety
- Review of incident trends or emerging risks
- Artificial Intelligence safeguards and privacy expectations

Training may occur through team meetings, professional development sessions or targeted briefings following any digital-related incident.

Monitoring, Evaluation, and Review Process

Monitoring

The Nominated Supervisor is responsible for monitoring the implementation of this policy in daily practice.

Monitoring will include:

- Oversight of compliance with personal electronic device restrictions
- Review and maintenance of the Electronic Device Register
- Oversight of authorised medical photographs and documentation processes
- Review of digital technology use within the educational program
- Monitoring of any online safety incidents, breaches or near misses

Monitoring may occur through routine supervision, staff discussions, incident review and internal audits.

Evaluation

The service will evaluate the effectiveness of this policy by:

- Reviewing incident data relating to digital technologies or online environments
- Reviewing trends in breaches, near misses or device misuse
- Considering feedback from educators, families and children
- Assessing whether identified risks are adequately controlled through current procedures

Evaluation findings will inform updates to training, risk assessments and operational practices.

Review

This policy will be formally reviewed at least every two years, or earlier if:

- legislation or regulations change,
- new technologies or platforms are introduced at the service, or
- incidents highlight gaps in practice.

All staff are consulted as part of the review process, and families are invited to contribute feedback.

The Approved Provider endorses all updates and ensures staff re-sign to confirm awareness.

The Digital Technologies and Online Environments Risk Assessment will also be reviewed annually and updated as required.