ADVENTURE OSHC

Safe Use of Digital Technologies and Online Environments Policy

National Quality Standard

Area 1 - Educational Program and Practice	
Standard 1.1	Program
Element 1.1.3	Program learning opportunities: All aspects of the program, including routines, are organised in ways that maximise opportunities for each child's learning.
Area 2 - Children's Health and Safety	
Standard 2.2	Safety
Element 2.2.1	Supervision: At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard
Element 2.2.3	Child Protection: Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk of abuse or neglect.

Children (Education and Care Services) National Regulations (2011 SI 653)

Reg. 73	Educational Program
Reg. 76	Information about educational program to be given to parents
Reg. 155	Interactions with children
Reg. 156	Relationships in groups
Reg. 181-184	Confidentiality of records and storage of records

Related Policies

Providing a Child Safe Environment Policy
Behaviour Guidance Policy
Child Protection Policy
Governance, Management and Record Keeping Policy

ADVENTURE OSHC

Links to the Child Safe Standards

Standard 1 – Child safety and wellbeing is embedded in organisational leadership, governance and culture	Adventure OSHC embeds child safety in every aspect of our digital technology practices. Our leadership team sets clear expectations for staff about the safe and appropriate use of technology, ensuring decisions always prioritise children's wellbeing. Educators model responsible use of technology, follow strict device security protocols, and receive regular training on child safe online practices.
Standard 2 – Children and young people are informed about their rights, participate in decisions affecting them and are taken seriously	We empower children to understand their right to be safe online and encourage them to speak up if they encounter anything that makes them feel uncomfortable. Educators involve children in developing service rules for digital technology use, ensure their views are respected, and act promptly on any concerns raised.
Standard 4 – Equity is upheld and diverse needs respected in policy and practice	Adventure OSHC ensures that technology use is inclusive and accessible for all children, including those with additional needs or from diverse cultural backgrounds. Educators adapt digital activities so that every child can participate safely and meaningfully, and they work with families to ensure individual requirements are met.
Standard 6 – Processes to respond to complaints and concerns are child focused	If a child raises a concern about technology use, unsafe online content, or inappropriate behaviour, educators respond immediately, focusing on the child's safety and wellbeing. We ensure children are supported, informed of the actions being taken, and involved in solutions where appropriate.
Standard 8 – Physical and online environments promote safety and wellbeing while minimising the opportunity for children to be harmed	We maintain strict supervision when children use digital technologies, select only age-appropriate and educational programs, and ensure all online activity occurs in open, visible areas. Educators' use of personal devices is tightly controlled, with exceptions only granted for essential purposes approved by the Approved Provider. All images and videos are taken only with consent, using service-issued devices, and stored securely.

ADVENTURE OSHC

Policy Statement:

Adventure OSHC values hands-on, social, and outdoor play. We recognise that digital technologies can enrich learning when used intentionally and safely. Our approach prioritises children's health, wellbeing, and protection from online harm, while modelling respectful digital citizenship.

We are committed to:

- Safeguarding children's privacy and digital rights.
- Preventing exposure to harmful or inappropriate online content.
- Supporting children to develop self-protection and digital literacy skills.
- Meeting all regulatory requirements under Reg 168 and the National Quality Standard.
- Following the **National Model Code for Taking Images and Videos of Children and the Child Safe Standards** to ensure dignity, safety, and respect.

Purpose:

This policy aims to:

- Promote the safe, responsible, and ethical use of digital technologies at Adventure OSHC.
- Protect children from harm in online environments and safeguard their personal information.
- Ensure all images, videos, and recordings are managed in line with the **National Model Code for Taking Images and Videos of Children (2024).**
- Define clear expectations for staff, children, and families regarding technology use.
- Establish procedures for risk assessment, incident management, and continuous improvement.

Scope:

This policy applies to all children, families, educators, management, and visitors to Adventure OSHC.

Definitions:

- **Digital technologies**: Tablets, laptops, smartwatches, cameras, projectors, robotics, interactive whiteboards, mobile phones.
- **Online environments**: Websites, apps, and platforms accessible via the internet.

- **Personal device**: Technology owned by an individual, such as a phone, tablet, laptop, or smartwatch.
- **Images/videos**: Photographs, film, or recordings in any format.
- **Digital incident**: Any event where a child is exposed to unsafe content, online harm, or inappropriate device use.

Implementation:

Guidelines for Use

General Principles	• Digital technologies are used only when they enhance the OSHC program or support wellbeing. • Outdoor play and social interaction are prioritised over screen time. • All child use of technology is actively supervised. • Only pre-approved, age-appropriate, educational programs or websites are used. • Educators will remind children that if they encounter anything online that makes them feel uncomfortable, scared, or upset, they can speak to a trusted adult. • **Closed-circuit television (CCTV)** or other optical surveillance devices are not used in any child-accessible areas of the service. Adventure OSHC prioritises active supervision and safe, transparent practices over surveillance technologies.
Children's Personal Devices	• Children are not permitted to use personal devices during OSHC sessions (before/after school care and vacation care). • All personal devices must be stored in the child's bag or in a location specified by the Coordinator or Responsible Person. **This includes smart watches.** **An exception may be approved for a child's personal device when it is required for a medical condition (e.g., diabetes monitoring), supported by documentation and authorised by the Approved Provider.**
Educator's Personal Devices	• Personal electronic devices capable of taking images or videos (such as tablets, mobile phones, digital cameras, and smartwatches), as well as personal storage or file transfer media (such as SD cards, USB drives, hard drives, and cloud storage), must not be in the possession of any educator while

	providing education and care and working directly with children. ● Any **exceptions** must be for **limited, essential purposes** and are **authorised in writing by the Approved Provider,** and such use must never impede the active supervision of children. **Authorised Essential Purposes** The Approved Provider authorises the use and possession of personal mobile phones and other personal electronic devices in the following circumstances: ● **Excursions** – educators may carry a personal mobile phone for essential communication, including emergencies, coordination of transport, contact with the service, or communication with parents/carers where service-issued devices are unavailable or non-functional. ● **Emergency communication** – e.g., a lost child, injury to a child or staff member, serious incident, lockdown, or evacuation. ● **Personal health requirements** – e.g., blood sugar monitoring or heart condition monitoring. ● **Disability-related needs** – where a device is an essential means of communication for an educator or staff member. ● **Family necessity** – e.g., urgent communication regarding an ill or dying family member. ● **Technology failure** – e.g., when a temporary outage of service-issued devices has occurred. ● **Local emergency event** – to receive critical updates from emergency services. When a personal device is used under one of these authorised purposes, it must be stored securely when not in use, remain inaccessible to children, and be used only for the authorised purpose.
Service-Issued Devices	Adventure OSHC ensures that all service-issued devices are configured, stored, and used in strict accordance with the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025. These controls are mandatory and apply to all mobile phones, tablets, laptops, cameras and any other device capable of taking, storing, or sending images, videos, or digital information.

Configuration Controls
All service-issued devices must meet the following configuration requirements:

- A secure passcode/PIN is enabled and known only to authorised staff.
- Auto-lock is activated and set to the shortest practical interval.
- AirDrop, Bluetooth sharing, hotspot and all peer-to-peer file-sharing functions are disabled.
- Access to personal accounts (e.g., iCloud, personal Google accounts, messaging apps, email) is removed.
- Only pre-approved, work-related apps and browsers are installed.
- Camera and photo storage settings comply with consent, privacy and storage requirements in this policy.
- Child-accessible apps, entertainment apps, social media and unapproved platforms are not installed.
- Notifications and message previews are restricted so no information is visible on a locked screen.
- The device is stored securely when not in use and remains inaccessible to children unless being intentionally used for a supervised learning experience.

Use of Service-Issued Devices

- Images and videos may only be taken on service-issued devices and only for purposes outlined in this policy.
- Files must be stored securely, password-protected, and deleted once no longer required for their original purpose.
- Files must not be transferred via AirDrop, personal email, personal cloud storage or to personal phone numbers.
- All transfers must occur through approved and secure organisational systems.

Configuration Declaration & Compliance Checks
Adventure OSHC completes and maintains a Service-Issued Device Configuration Declaration for every device. This declaration confirms that the device meets all required configuration controls and is reviewed:

- When the device is first issued
- At least monthly as part of the service's digital compliance

	check ● Annually during the re-declaration stage The Approved Provider (or their delegate) will sight and approve each completed declaration. Any device found to be non-compliant must be removed from use until all configuration requirements are met. **Educator Responsibilities** Educators must use service-issued devices only for legitimate work purposes, follow all configuration and storage requirements, and report any concerns, faults, breaches or suspected misuse immediately to the Nominated Supervisor.
Use of Images and Videos	**Consent** ● Written, informed consent from families is required before any images/videos of children are taken. ● Consent may be withdrawn at any time and must be respected immediately. ● Children's own views will be sought and respected, even where family consent exists. **Child Participation** ● Children will be asked if they are comfortable before any image/video is taken. ● If a child refuses or shows discomfort, no image/video will be taken. **Purpose** Images/videos may only be taken for: ● Educational documentation (e.g., MTOP programming). ● Compliance (e.g., incident reports, risk assessments). ● Service promotion (only with separate written family consent). ● Casual or recreational photography by staff is prohibited. **Restrictions** ● No images/videos will be taken in private or sensitive areas (bathrooms, change rooms, rest spaces). ● Children will not be depicted in unsafe, demeaning, or disrespectful ways.

	Storage, Retention, and Disposal ● All images/videos are taken only on service-issued devices. ● Files are password-protected, securely stored, and access is limited to authorised staff. ● Images/videos are retained only for as long as required for their original purpose, then securely deleted. ● Staff leaving the service must not retain any images/videos of children. **Publishing and Sharing** ● No images/videos are published or shared without separate written family consent. ● Safety, dignity, and wellbeing are prioritised in all publications. ● No child's full name will be published alongside their image/video. **Breaches and Complaints** ● Any breach (unauthorised images, misuse, data leaks) is treated as a serious incident. ● Breaches are reported immediately, documented, reviewed by management, and communicated to families. ● Complaints follow the service's Complaints Policy and are child-focused. ● Breaches may result in disciplinary action under service HR procedures.
Online Safety	● Filters and restrictions applied to all service devices. ● Children are reminded to speak up if they see unsafe or upsetting content. ● No personal information is published online without written family consent.
Risk Assessments	A documented risk assessment will be conducted: ● Annually, ● Before introducing new digital technologies or platforms, and ● After digital incidents. Risk assessments will cover supervision, privacy, device security, exposure risks, inclusion, and accessibility.

ADVENTURE OSHC

Incident Management	All digital incidents (unsafe content, cyberbullying, consent breaches) are: ● Reported immediately to the Nominated Supervisor ● Recorded in the compliance system (e.g., 1Place) ● Reviewed by management ● Communicated to families as appropriate. ● Learnings inform staff training and policy review.
Data Security and Third-Party Apps	● Only vetted, secure platforms are used (e.g., Xplor). ● Unapproved apps or websites are prohibited. ● Confidential data complies with Regs 181–184.

Roles and Responsibilities

Management	● Ensure all staff understand and follow this policy. ● Provide ongoing training on safe digital technology use and online safety. ● Maintain secure storage of images/videos and ensure password protection on all service devices. ● Monitor and review technology use regularly.
Educators	● Model respectful and safe technology use. ● Supervise all child use of digital technologies. ● Follow image/video consent requirements. ● Report and respond to breaches or online safety incidents immediately.
Families	● Support the service's guidelines by reinforcing them with their children. ● Provide or withdraw consent for images/videos in writing. ● Raise concerns about technology use promptly with the Coordinator.
Children	● Follow service technology rules. ● Report unsafe or uncomfortable online experiences.

ADVENTURE OSHC

Governance and Review

- Policy reviewed annually, or earlier if new risks, technologies, or laws arise.
- Reviews include input from children, families, and educators.
- Updates are shared with families in writing.

Sources

- Education and Care Services National Regulations (2011 SI 653)
- National Quality Standards
- Child Safe Standards
- National Model Code
- Information Sheet - NQF Child Safety Changes from 1 September 2025 and 1 January 2026
- ACECQA Policy Guidelines - Safe Use of Digital Technologies and Online Environments
- Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025

Version control created	August 2025 (GW)
Reviewed	Nov 2025 - Service-issued device updated to include device configuration declaration (GW)
Reviewed	February 2026 - interim laptop use section added (GW)
Reviewed	April 2026 - interim laptop use section removed (GW)
Next review	October 2026

ADVENTURE OSHC

Compliance Mapping Table

Requirement Source	Expectation / Obligation	Policy Section(s)	How Policy Addresses It
National Regulations – Reg. 73	Educational program must be delivered in a way that contributes to learning and development.	General Principles, Purpose	Policy ensures digital technologies are used only when they enhance the OSHC program and learning outcomes.
National Regulations – Reg. 76	Information about the educational program must be given to parents.	Governance & Review; Families Responsibilities	Families are informed about technology use, consent processes, and policy updates.
National Regulations – Reg. 155	Interactions with children must be respectful and support wellbeing and learning.	General Principles, Child Participation	Policy ensures children are involved in rule-setting and treated respectfully in all technology use.
National Regulations – Reg. 156	Relationships in groups must be positive and promote inclusion.	Child Participation, Online Safety	Policy requires safe, supervised group use of digital technologies with inclusion of all children.
National Regulations – Reg. 168(2)(ga)	Services must have a policy on the safe use of digital technologies and online environments.	Whole Policy	This policy fulfils the new mandatory requirement (July 2025).
National Regulations – Regs. 181–184	Records must be kept secure and confidential.	Storage, Retention & Disposal; Data Security	Policy requires password protection, secure storage, restricted access, and disposal of files.

ADVENTURE OSHC

National Regulations – Reg. 101 (applied)	Risk assessments must be conducted before excursions (principle extended to digital environments).	Risk Assessments	Policy requires documented digital risk assessments annually, before new tech, and after incidents.
NQS QA1: Educational Program	1.1.3 – Program learning opportunities must maximise children's learning.	General Principles, Purpose	Policy ensures technology use is intentional, educational, and limited.
NQS QA2: Children's Health & Safety	2.2.1 – Supervision; 2.2.3 – Child Protection.	Supervision, Online Safety, Incident Management	Policy ensures children are supervised, protected from harm, and staff are trained in child protection obligations.
NQS QA7: Governance & Leadership	7.1.2 – Systems must support risk management and continuous improvement.	Governance & Review	Policy sets review cycles, consultation with families/children, and continuous improvement processes.
Child Safe Standard 1	Child safety and wellbeing is embedded in organisational leadership, governance and culture.	Policy Statement, Management Responsibilities	Policy commits leadership to embed child safety in digital practices.
Child Safe Standard 2	Children are informed about their rights, participate in decisions, and are taken seriously.	Child Participation; Consent	Policy ensures children are asked and respected each time images/videos are taken.
Child Safe Standard 4	Equity is upheld and diverse needs respected.	General Principles, Online Safety	Policy adapts tech use to include all children, regardless of needs or background.

ADVENTURE OSHC

Child Safe Standard 6	Processes for complaints and concerns are child-focused.	Breaches & Complaints; Incident Management	Policy ensures child safety is prioritised in digital complaints and breaches.
Child Safe Standard 8	Physical and online environments promote safety and wellbeing.	Supervision, Restrictions, Online Safety	Policy ensures all digital environments are supervised, safe, and inclusive.
National Model Code (2024) – Part 1	Only service-issued electronic devices should be used when taking, sending or storing images or videos of children.	Use of Images & Videos – Service Devices Only	Policy requires only service-issued devices be used for photos/videos; personal devices not permitted.
Model Code – Part 2	Personal devices… should not be in possession while working directly with children, except for limited, essential authorised purposes.	Educators' Personal Devices	Policy prohibits staff personal devices during care, with only essential authorised exceptions.
Model Code – Part 3	Essential purposes include emergencies, personal health, disability communication, family necessity, device failure, or local emergency warnings.	Authorised Essential Purposes	Policy lists these exact scenarios as permitted exceptions.
Model Code – Part 4	Approved providers must have strict controls for storage and retention of images/videos of children.	Storage, Retention & Disposal	Policy requires password protection, secure storage, restricted access, and deletion of files.
ACECQA Guidelines (2025) – Consent	Services must obtain informed, written parental consent before taking images/videos;	Use of Images & Videos – Consent	Policy requires written consent, withdrawal at any time, and respect for children's own views.

	families may withdraw consent at any time.		
Guidelines – Child Participation	Children's views must be sought and respected, even if families have given consent.	Child Participation	Policy requires children to be asked each time; refusal respected even with family consent.
Guidelines – Legitimate Purpose	Images/videos may only be taken for legitimate purposes: documenting learning, compliance, or promotion with explicit consent.	Use of Images & Videos – Purpose	Policy limits use to educational, compliance, or consented promotion; bans casual photography.
Guidelines – Prohibited Practices	Images/videos must never be taken in private or sensitive spaces (bathrooms, change rooms, rest areas).	Use of Images & Videos – Restrictions	Policy bans photos/videos in private or sensitive areas, or those compromising dignity.
Guidelines – Secure Storage	Images/videos must be securely stored, password-protected, access-limited, and deleted when no longer required.	Storage, Retention & Disposal; Data Security	Policy requires service devices only, secure storage, restricted access, and disposal.
Guidelines – Publishing	Images/videos must not be published without additional explicit family consent. Full names must never be published with images.	Publishing & Sharing	Policy requires separate consent for publishing and bans linking names with images.
Guidelines – Breach Response	Any breach or misuse must be treated as a serious incident, reported, investigated, and communicated to families.	Breaches & Complaints; Incident Management	Policy requires reporting, recording in compliance system, informing families, and review.