SAFE USE OF DIGITAL TECHNOLOGIES & ONLINE ENVIRONMENTS POLICY

Policy Statement

At Fun 4 U Helensburgh our Out of School Hours Care (OSHC), we are committed to ensuring the safe and responsible use of digital technologies and online environments within our service. We recognise the value of digital tools in supporting learning, communication, and creativity, while also prioritising the protection of children's safety, privacy, and wellbeing. This policy establishes clear guidelines for educators, children, families, and visitors around the appropriate and secure use of technologies and online platforms, in line with our duty of care, National Regulations, and the National Principles for Child Safe Organisations (Reg 168). We aim to foster a culture of cyber safety, informed consent, and respectful digital practices across all aspects of our service operations.

Background

Digital technologies and online environments are increasingly used in education and OSHC services to support programming, documentation, communication, and children's learning experiences. While these tools offer valuable opportunities, they also introduce potential risks related to privacy breaches, inappropriate content, overexposure, and misuse of images or data. Children have the right to be safe and protected, including in digital spaces. It is therefore essential that OSHC services implement robust strategies to manage the collection, storage, and sharing of digital content, ensure informed consent from families, and promote cyber safety practices for children and staff. (Reg 168 (h))

This policy reflects current best practice and aligns with the:

- National Quality Framework (NQF)
- Education and Care Services National Law and Regulations
- National Model Code for Taking Images or Videos of Children
- My Time, Our Place Framework
- Child Safe Standards

Through careful planning, communication, and monitoring, we strive to provide a safe and developmentally appropriate digital environment that supports children's and young people's wellbeing, agency, and learning.

Legislative Requirements and links to the National Quality Framework

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2	Safety	Each child is respected.
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 (effective January 2026)	Management, educators and staff are aware of their roles and responsibilities regarding child safety, including the need to identify and respond to every child at risk of abuse or neglect
QUALITY AREA 4: STAFFING ARRANGEMENTS		
4.2.2	Professional standards	Professional standards guide practice, interactions and relationships.
QUALITY AREA 5: RELATIONSHIPS WITH CHILDREN		
5.1	Relationships between educators and children	Respectful and equitable relationships are maintained with each child.
5.1.2	Dignity and rights of the child	The dignity and rights of every child are maintained.
QUALITY AREA 7: GOVERNANCE AND LEADERSHIP		
7.1.2	Management System	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 AND NATIONAL REGULATIONS	
S.162A	Child protection training
S.165	Offence to inadequately supervise children
S.167	Offence relating to protection of children from harm and hazards
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
168	Education and care service must have policies and procedures
168 (h)	Providing a child safe environment, including matters relating to; (i) the promotion of a culture of child safety and wellbeing within the service; and (ii) the safe use of online environments at the service;
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 approved provider
183	Storage of records and other documents
184	Storage of records after service approval transferred

Legislation

- A New Tax System (Family Assistance) Act 1999
- Child Care Subsidy Secretary's Rules 2017
- Family Law Act 1975
- Privacy Act 1988 (the Act)
- Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook.

Definitions of Key Terms used in the Policy

TERM	MEANING	SOURCE
ACECQA – Australian Children's Education and Care Quality Authority	The independent national authority that works with all regulatory authorities to administer the National Quality Framework, including the provision of guidance, resources, and services to support the sector to improve outcomes for children.	ACEQA
Artificial Intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given sent of human defined objectives or parameters without explicit programming.	NQF Online Safety Guide_1.pdf
Cyberbullying	Cyberbullying can be described as any repeated harassment, insults and humiliation that occurs through electronic mediums such as email, smartphones, social networking sites, instant messaging programs, chat rooms, web-sites and through the playing of online games. Cyberbullying is not one isolated nasty comment or post but a repeated action.	Review into the non-educational use of mobile devices in NSW schools – report
Cybersafety	The safe, responsible and informed use of digital media and technology. It is about keeping information safe and secure but also about being responsible with that information and being respectful of other people online.	Review into the non-educational use of mobile devices in NSW schools – report
Disclosure	Process by which a child conveys or attempts to convey that they are being or have been sexually abuses, or by which an adult conveys or attempts to convey that they were sexually abused as a child	NQF Online Safety Guide_1.pdf
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	NQF Online Safety Guide_1.pdf
ICT	Information and Communication Technologies	NQF Online Safety Guide_1.pdf
Illegal content	Includes: images and videos of child sexual abuse, Content that advocates terrorist acts, Content that promotes, incites or instructs in crim or violence and footage of real violence, cruelty and criminal activity.	NQF Online Safety Guide_1.pdf
Optical Surveillance	Has the same meaning as in section 6(1) of the Surveillance Devices Act 2004 of the Commonwealth	NQF Online Safety Guide_1.pdf
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender	NQF Online Safety Guide_1.pdf

Smart Toys	Smart toys generally require an internet connection to operate as the computing task is on a central server.	NQF Online Safety Guide_1.pdf
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	NQF Online Safety Guide_1.pdf
Unwanted Contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed	NQF Online Safety Guide_1.pdf

Implementation of the Principles that Inform the Policy

At Fun 4 U Helensburgh, digital technology and electronic devices are integrated thoughtfully into our service to enhance learning programs (Reg. 73), communication, documentation, and administration. These tools are used to support children's engagement in age-appropriate activities, record and share their development and achievements, communicate effectively with families, streamline sign-in and sign-out processes, and assist educators with planning and service management (Reg 76).

Our educators ensure that all digital technology use within the service aligns with child safety principles and is appropriate to each child's age, developmental stage, and individual needs. Within our program we do not allow Children access to online content through our service-issued devices, this is in place to ensure cyber safety and prevent access to inappropriate or harmful material. All use of technology by staff, volunteers, and children complies with our policies on confidentiality, mobile device usage and privacy. We promote responsible digital citizenship and model respectful, safe online behaviours for the children in our care (Reg 155).

Digital Technology and Electronic Devices Used at Fun 4 U

Fun 4 U follows the National Model Code and Guidelines for taking images or videos of children. While currently optional, it is anticipated that legislation will soon require all OSHC services to ban personal electronic devices capable of capturing images or videos, with breaches attracting fines. For example, services in Victoria are already prohibited from using or possessing such devices as of 26 September.

The Approved Provider will inform all staff, educators, visitors, volunteers, and families that the use of personal electronic devices to take photos, record audio, or capture video of children attending our OSHC Service is strictly prohibited. This includes, but is not limited to:

- Mobile phones and tablets
- Digital cameras and video recorders
- Smart watches and wearable technology
- Television
- META (Ray-Ban) sunglasses or similar devices
- Personal storage or file transfer devices (e.g. SD cards, USB drives, hard drives, cloud storage accounts)

Personal devices capable of capturing or storing images must not be in the possession of staff, educators, or visitors while working directly with children.

Electronic devices owned by the OSHC Service must not be removed from the premises, as they may contain personal or confidential information (e.g. staff or child details, photos, or videos). Exceptions may only be made where devices are required for operational purposes, such as excursions or transportation.

Exemptions

The Approved Provider may grant written exemptions for possession of a personal electronic device if it is required for:

- Emergency communication (e.g. lost child, injury, lockdown, evacuation)
- Personal health needs (e.g. heart or blood sugar monitoring)
- Disability-related communication support
- Urgent family matters (e.g. critically ill or dying family member)
- Receiving alerts during a local emergency (e.g. bushfire, evacuation notifications)

Even when an exemption is granted, personal devices must never be used to take images, videos, or audio recordings of children.

Device Register

Our OSHC Service will maintain a register of all service-owned electronic devices. This register will include:

- Device type and description
- Date of purchase
- Intended use and assigned user (if applicable)
- Security and password settings
- Recording, connectivity, and storage features

The register may include, but is not limited to:

- Computers and tablets
- Mobile phones
- Cameras and audio recorders
- Smart toys and internet-connected devices

Children's Devices

Children enrolled at our OSHC Service are not permitted to bring personal electronic devices to the service unless an exemption is approved by the Approved Provider or Nominated Supervisor for a diagnosed medical condition or disability. If a child brings an electronic device without authorisation, it will be switched off and securely stored in a locked cupboard until collection as per our Mobile Device Usage Policy.

Parents's & Care Givers Devices

Our OSHC Service is committed to providing a safe physical and digital environment for all children. To support this, parents, guardians and authorised persons must adhere to the following requirements when attending the service:

- Personal mobile devices and other electronic devices must not be used within the service premises during drop-off and collection times.
- Parents and authorised persons must not take photos, videos, or audio

recordings of children, staff or the service environment at any time.

- The use of devices in the service environment is restricted to prevent breaches of privacy, unauthorised sharing of images, and potential risks to child safety.
- Parents and authorised persons are expected to model appropriate and respectful use of technology in line with the service's child safe practices.

By limiting the use of personal devices within the service, we ensure:

- Children's rights to privacy and safety are upheld
- The risk of unauthorised recording or sharing of images is minimised
- A focused and safe environment is maintained during high-risk transition times

Any concerns regarding digital safety or breaches of this policy will be managed in accordance with the service's Child Safe Environment and Complaints policies.

Screen Time

At Fun 4 U OSHC, screen time is used purposefully and in moderation to support the educational program and enhance children's learning experiences. Digital technology may be incorporated into activities for creative projects, research, or group learning (Reg 156), but is never used as a substitute for active play, social interaction, or hands-on exploration. We follow Australia's Physical Activity and Sedentary Behaviour Guidelines, ensuring children aged 5–12 years limit recreational screen time to no more than two hours per day, and screen use is not offered as a reward or behaviour management tool. Screen-based activities are always supervised by educators, take place in open, visible spaces, and are limited to age-appropriate content on service-issued devices. The Television is used during some afternoon programs for the children to watch appropriate and approved movies, however staff will ensure it is turned off for periods of time during the session to encourage children to participate in the other activities available to them. Moreover it is important to note on days when the weather conditions pose a risk to the children's safety and prevent use of the outside space such as a heatwave or rain, the television is left on for longer periods to accommodate for the increase of children inside. This practice occurs on the very rare occasion, is decided by the approved

provider/management/nominated supervisor on the day and is constantly reviewed throughout the session to endure adequate breaks are maintained. Our approach aims to promote a healthy balance between technology use and active, engaging play in a safe and supportive environment.

Software Programs and Apps Utilised at Fun 4 U

Our OSHC Service uses a range of secure, service-issued software programs and applications to support both the educational program and the effective administration of the service. All apps and programs accessed by staff, educators, visitors, and children are carefully vetted, regularly reviewed, and updated with the latest security and system upgrades.

Access to these platforms is password protected to safeguard the privacy and confidentiality of children, families, and staff. Each authorised user is assigned an individual login and must ensure their account and password details remain private and are never shared.

The Approved Provider will ensure that any programs requiring additional security clearance, such as Child Care Subsidy (CCS) software, are only accessed by authorised personnel who have completed the necessary screening in accordance with Family Assistance

Artificial Intelligence (AI) Interactions and Guidelines

At our OSHC Service, educators and staff who choose to use Artificial Intelligence (AI) tools must be mindful of their limitations, potential privacy risks, and the possibility of inaccuracies in the information provided. AI may be used to support and assist with documentation, creativity and planning; however, it is the responsibility of the educator or staff member to verify the accuracy of any content generated and not rely on AI as a sole or authoritative source.

All input into AI tools must be original work, and any output must be carefully reviewed to ensure it is factually correct, contextually relevant, and aligns with our service

philosophy, policies, and procedures.

Privacy and confidentiality are paramount. Staff must never enter information that could directly or indirectly identify individual children, families, or staff members, including names, dates of birth, addresses, photographs, or any other personal or sensitive data.

By following these guidelines, we ensure that AI is used responsibly and in a way that supports high-quality education and care while maintaining our strong commitment to child safety and privacy.

Capturing Images and Videos During the hours of our OSHC service

The Approved Provider is responsible for determining who is authorised to capture, use, store, and delete images or videos of children using Fun 4 U's Service–issued digital devices.

All images and videos:

- Must be stored securely with password protection
- Must only be accessed by authorised personnel
- Must be taken and used in line with our services policies
- Must have a clear, appropriate, and documented purpose that supports children's learning, wellbeing, and right to privacy.
- Only the children and young persons who

Educators will engage in professional discussions to assess the intent, appropriateness, context, and consent before capturing and using any images or videos.

Fun 4 U will regularly review the security and storage of all digital data, including images and videos of children. Monthly backups will be conducted and stored securely, either offline or on a secure cloud-based service.

Digital data will be destroyed in line with our Record Keeping and Retention Policy and procedure. Under no circumstances are staff, educators, visitors, or volunteers permitted to transfer images or videos from OSHC Service devices to personal devices. Any

unauthorised transfer of digital data may result in disciplinary action.

Confidentiality and Privacy

Our Privacy and Confidentiality Policy applies to all uses of digital technology and online environments within our OSHC Service. All staff, educators, and visitors must ensure that any information, images, or digital content relating to children, families, or the Service is collected, stored, used, and shared in line with relevant privacy legislation (Reg. 84), Service policies, and procedures, to maintain confidentiality and protect children's safety and wellbeing. (Reg 181, 184 &185)

The Nominated Supervisor must promptly inform the Approved Provider of any suspected or actual security threat, or unauthorised access to sensitive information. Our OSHC Service will follow the practices outlined in the Safe Use of Digital Technologies and Online Environments Procedure to safeguard all personal and sensitive data.

In the event of a possible data breach, the Approved Provider will notify the Office of the Australian Information Commissioner (OAIC) using the Notifiable Data Breach Form. A reportable breach may include (but is not limited to):

- Loss or theft of a device containing personal information about children or families (e.g. parent names, contact numbers, dates of birth, allergy records)
- Hacking of a database containing personal or sensitive child/family information
- Personal information being mistakenly shared with an unauthorised person (e.g. portfolios, developmental reports)
- Any loss or unauthorised access to a device containing personal information while on an excursion

All educators must be aware of their mandatory reporting requirements and immediately report any concerns relating to child safety, including inappropriate or unsafe use of digital technology, to the Approved Provider or Nominated Supervisor.

Identification and Reporting of Online Abuse and Safety Concerns

Our OSHC Service is committed to implementing measures that protect children when using digital technology and accessing online environments.

The Approved Provider, Nominated Supervisor, and Management will:

- Ensure all staff, educators, students, and volunteers are aware of their mandatory reporting obligations and promptly report any concerns about child safety—including the inappropriate use of digital technology—to the Approved Provider or Nominated Supervisor. *(Refer to the Child Protection Policy)*
- Support educators to:
    - Encourage children to seek help if they encounter anything unexpected online that makes them feel uncomfortable, scared, or upset
    - Listen sensitively and respond appropriately to any disclosures from children regarding unsafe online interactions or exposure to inappropriate content, following the Child Protection Policy, Behaviour Guidance: Bullying Policy, and relevant reporting procedures
    - Respond to and report any breaches or incidents involving the inappropriate use of digital devices or online services to management
- Ensure all concerns are documented, addressed promptly, and followed up appropriately, with necessary support provided to the child and their family
- Report any suspected cases of online abuse to the relevant authorities, including the eSafety Commissioner and Police, in line with legal obligations and child protection procedures
- Notify the Regulatory Authority via NQAITS within 24 hours if a child is involved in a serious incident related to unsafe online interactions, exposure to inappropriate content, or suspected online abuse

Cyber Safety Education

1. Children will participate in age-appropriate discussions and activities about:
    - Online safety and respectful digital behaviour

- The importance of switching off and engaging in real-world play
- The risks of sharing personal information online
- What is cyberbullying and cybersafety

2. Resources from the eSafety Commissioner will be incorporated into programming as part of our ongoing commitment to child safety.

Staff's Personal Technology Devices

Staff, educators, students, volunteers, and visitors are not permitted to use personal electronic devices—such as mobile phones, tablets, smart watches, digital cameras, META sunglasses, or other recording-capable devices—while working directly with children at the OSHC Service.

- Personal devices must be stored securely in a designated area during work hours and may only be accessed during scheduled breaks in areas where children are not present.
- Personal devices are strictly prohibited for taking images, videos, or audio recordings of children under any circumstances.
- Accessing social media, personal emails, or other non-work-related content on personal devices is not permitted during work hours.
- The OSHC Service accepts no responsibility for the loss, theft, or damage of personal devices brought to the workplace.

Exemption of Personal Devices

In certain circumstances, the Approved Provider or Nominated Supervisor may grant a written exemption allowing the use or possession of a personal electronic device while at the OSHC Service.

- Exemptions must be requested in writing and approved before the device is brought into a child-accessible area.
- Even where an exemption is granted, personal devices must never be used to take images, videos, or audio recordings of children.
- Exemptions may be granted for:
    - Emergency communication during incidents such as a lost child, injury, lockdown, or evacuation.

    - Personal health needs, such as medical monitoring for heart conditions or diabetes.
    - Disability-related communication or accessibility requirements.
    - Urgent family matters, such as a critically ill or dying family member.
    - Local emergency alerts, such as bushfire, flood, or evacuation warnings.
- The Approved Provider will maintain a confidential register of all exemptions granted, including the staff member's name, reason for exemption, and duration.
- Any breach of the exemption conditions will result in immediate withdrawal of the exemption and may lead to disciplinary action.

The approved provider/management/nominated supervisor will ensure:

- Compliance with all obligations under the Education and Care Services National Law and National Regulations.
- All educators, staff, students, visitors, and volunteers understand and adhere to this policy and its associated procedures.
- New employees, students, and volunteers receive a copy of this policy during induction and are shown where it can be accessed.
- Families are made aware of this policy and procedure at enrolment and informed where it can be accessed.
- A strong child-safe culture is promoted and maintained, in line with the Child Safe Environment Policy, Child Protection Policy, and the National Principles for Child Safe Organisations (or state-specific standards).
- All staff, educators, volunteers, and students are aware of current child protection laws and their duty of care to take reasonable steps to prevent harm to children.
- Ongoing professional learning is provided to staff regarding safe and responsible use of digital technologies and online environments.
- An Electronic Device Register is developed and maintained for all OSHC Service-issued devices, including details of purchase, configuration, and assigned users.
- Appropriate educator-to-child ratios (Reg 122 & 123) and active supervision are maintained at all times when children are using digital technology or accessing online environments (Reg S.165)

- Students, volunteers, and visitors are never left alone with children.
- The National Model Code for taking images and videos of children is followed, including:
    i) Prohibiting the use of personal devices for capturing images or videos when working directly with children.
    ii) Allowing only OSHC Service-issued devices to be used for this purpose.
    iii) Ensuring Service devices are securely configured and maintained to prevent unauthorised access.
    iv) Requiring written parental authorisation before visitors or professionals (e.g., NDIS or inclusion support staff) capture images or video of children.
- A clear complaints process is in place for children, educators, and families to raise concerns (see Dealing with Complaints Policy).
- The Privacy and Confidentiality Policy is adhered to at all times.
- Written authorisation is obtained from families before taking, using, storing, or destroying images/videos of children, or allowing children to use electronic devices.
- Families are informed of their right to withdraw authorisation in writing, and any associated images/videos are deleted or destroyed when this occurs.
- Digital data is stored securely—both online and offline—and archived regularly (monthly recommended).
- Images and videos are retained in line with the Record Keeping and Retention Policy (minimum three years after last attendance).
- External experts are consulted if online abuse, cyberbullying, or digital safety risks are identified.
- Policies and procedures reflect equity, diversity, and children's privacy, and empower children to participate safely online.
- Annual (or as needed) risk assessments are conducted on the use of digital technologies and online environments.
- Anti-virus and internet security systems (including firewalls) are installed and maintained.

- Educators are aware of and follow screen-time guidelines from Australia's Physical Activity and Sedentary Behaviour Guidelines (no more than 2 hours entertainment screen time per day for 5–12 year olds), and this information is shared with families.

Educators will:

- Adhere to this policy and procedures at all times. (Reg 170)
- Participate in training on digital safety, privacy, and responsible use of technology.
- Actively supervise children when using devices connected to the internet.
- Model and promote a culture of child safety and wellbeing in digital environments.
- Never use personal electronic devices for capturing images, accessing social media, or breaching privacy while at the OSHC Service.
- Keep passwords secure and log out of devices after use.
- Seek permission before photographing children with Fun 4 U devices and explain to children how the images will be used.
- Never share identifiable personal information about children online.
- Avoid using screen time as a reward or behaviour management strategy.
- Introduce and reinforce age-appropriate online safety concepts through guidance, discussions, and activities.
- Consult with children about digital technology use to ensure their views are respected

Students and Volunteers (Reg 149) will:

- Follow the policy and procedures at all times.
- Not use personal devices to capture images, videos, or audio of children.
- Report any concerns about digital safety to the Approved Provider or Nominated Supervisor.
- Obtain written parental consent before capturing images/videos for documentation purposes (where applicable)

Families will:

- Follow the policy and procedures.
- Not use personal devices to capture images, videos, or audio of children while at the OSHC Service.

- Understand that their child's images may sometimes include other children, and agree not to share these online or beyond close family.

Considerations for Supervision

High Risk Behaviours

Fun 4 U recognises that online environments present potential risks to children's safety and wellbeing. To minimise these risks, educators maintain vigilant, active supervision whenever children access digital devices. We are particularly alert to the following high-risk behaviours:

- Sexting, Illegal content, uploading or sharing private information, images or videos.
- Accessing or engaging with inappropriate content, whether accidentally or intentionally.
- Making unauthorised in-app purchases or other financial transactions.
- Communicating with unsafe or unknown individuals, including unwanted contact

Our staff will intervene immediately if they observe unsafe behaviour, unsafe content, or signs of online grooming, cyberbullying, or exposure to harmful material. We take a proactive, supportive approach—encouraging children to seek help and ask questions without fear of blame or punishment. (Reg 12)

Physical Environment and Supervision

The Approved Provider, Nominated Supervisor, Management, Staff, Volunteers and Students will ensure the physical environment supports safe and transparent use of digital technologies by:

- Active Supervision
    - Children are never left unattended while using a device connected to the internet.
    - Approved devices are only used in open, visible areas where educators can always observe and monitor usage.
    - Educators maintain line-of-sight supervision and position themselves so they can see both the device screen and the child's surroundings.
    - Supervision responsibilities are shared, ensuring staff can observe one another and avoid blind spots.

- Environmental Design (Reg. 115)
    - The layout of indoor spaces is regularly reviewed to ensure visibility and reduce hidden areas where children might use devices unsupervised.
    - Digital device stations are placed in locations visible to multiple staff members.
    - Regular audits are conducted to identify and address any physical or procedural risks.
- Security Measures
    - All service-issued devices are password-protected and accessible to staff only.
    - Visitors and volunteers are always supervised when in areas where children use digital devices.
    - Children's use of personal devices is subject to our Mobile Device Usage Policy, and exemptions are documented in enrolment records if required for disability or medical support.
- Off-Site Use
    - If digital devices are used during excursions, transitions, or transportation, the same supervision and safety protocols apply as in the service environment.

Breach of policy

What is a breach of policy?

A breach is any action or inaction by any individual within the Service, including children and young people, that fails to comply with any part of the policy.

Managing a breach of the Mobile Device Policy

Management will address any breaches of this policy in a fair, impartial, and supportive manner. At Fun 4 U OSHC, any breach of the Safe Use of Digital Technologies and Online Environments Policy will be taken seriously to ensure the safety, wellbeing, and privacy of all children, families, and staff.

1. Identification of a Breach

- A breach may include, but is not limited to:
    - Use of personal devices to capture images, audio, or video of children.
    - Accessing inappropriate or unapproved online content.

    - Sharing personal or sensitive information without authorisation.
    - Failing to follow approved supervision procedures during technology use.
- Any staff member, educator, volunteer, visitor, or family member who becomes aware of a breach must report it immediately to the nominated supervisor or approved provider.

2. Immediate Response

- The nominated supervisor/management will take prompt action to stop the breach and secure any devices or materials involved.
- If children are at immediate risk, appropriate protective measures will be put in place, including removing access to the device and ensuring the child is supported.

3. Investigation

- An internal investigation will be conducted to gather facts, review evidence, and speak to all relevant parties.
- The investigation will assess the severity, intent, and impact of the breach, including whether privacy or child safety laws have been violated.

4. Notification

- Where required, the approved provider will notify the:
    - Regulatory Authority (within 24 hours if it constitutes a serious incident) via NQAITS. (Reg 175 & 176)
    - Office of the Australian Information Commissioner (OAIC) if there is a notifiable data breach.
    - eSafety Commissioner or Police for any suspected online abuse, exploitation, or illegal activity.
- Families will be informed if the breach involves their child's personal information or digital content.

5. Corrective Actions

- Breaches by staff or educators may result in disciplinary action, up to and including termination of employment, depending on the seriousness of the breach.
- Visitors or volunteers who breach the policy may have their access to the service revoked.
- Children involved in a breach will be supported through guidance, education, and behaviour management strategies in line with our Behaviour Guidance Policy.

6. Review and Prevention

- Following a breach, the service will review relevant policies, procedures, and practices to identify improvements.
- Additional staff training will be provided where required.
- Risk assessments relating to the use of digital technologies and online environments will be updated.

Induction and Training

At Fun 4 U OSHC, we are committed to ensuring all staff, educators, volunteers, students, and management understand their roles and responsibilities in maintaining a safe and secure digital and online environment. To uphold best practices and meet the National Regulation (S. 162A), all educators at Fun 4 U are required to complete approved child protection training through a registered training organisation. To stay informed and compliant, educators will also complete annual Child Protection Awareness Training to maintain up-to-date knowledge of child safety and mandatory reporting responsibilities.

Induction Training

- All new staff, educators, students, and volunteers will receive induction training prior to commencing duties.
- The induction will include:
    - An overview of the Safe Use of Digital Technologies and Online Environments Policy, Mobile Device Usage Policy and associated procedures.
    - Privacy and Confidentiality requirements, including the safe handling of personal and sensitive information.
    - The National Principles for Child Safe Organisations and child protection obligations.
    - Appropriate supervision practices for online activities and safe use of technology.
    - The National Model Code and Guidelines for taking images or video of children.
    - Breach management and reporting processes.
- Induction will also include practical demonstrations of service-issued devices, software platforms, and security procedures.

- All participants must sign an Acknowledgement of Understanding confirming they have read, understood, and agree to comply with the policy.

Ongoing Training and Information Sharing

- Refresher training will be provided to all staff and educators at least annually, or sooner if there are changes in legislation, policy, or technology.
- Topics may include:
    - Cyber safety awareness and emerging risks.
    - Updated guidance from the eSafety Commissioner and relevant authorities.
    - Changes to privacy laws and data protection practices.
    - New digital tools or systems introduced at the service.
- Digital safety and supervision strategies will be a standing agenda item at team meetings to encourage continuous discussion and problem-solving.
- Staff will be informed of any updates to policies and procedures promptly, with revised documents made easily accessible.
- External professional development opportunities will be promoted and supported to build digital literacy and online safety capabilities.

Monitoring Evaluation and Review

Fun 4 U, we proactively monitor updates from ACECQA and Childcare Centre Desktop to ensure our *Safe Use of Digital Technologies and Online Environments Policy* remains current and compliant. The policy is reviewed at least annually, in consultation with families, staff, educators, and management, to reflect best practices and evolving regulatory requirements. In addition to this, our policies are made readily available to families on our Facebook page and next to our sign in and out register we have a folder with a QR code to each policy. (Reg 171 & 172)

Links to other policies

Related Fun 4 U Polices	Child Care Centre Desktop Polices
Child Protection Policy Complaints Policy Excursions and Incursion Policy	Mobile Device Usage Policy Child Protection Policy Child Safe Environment Policy

Governance and Management of the Service including Confidentiality of Records Interactions with Children Policy Mobile Device Usage Policy Privacy Collection Statement Privacy and Confidentiality Policy Providing a Child Safe Environment Policy Safe use of Digital Technologies and Online Staff Code of Conduct Policy Supervision Policy	Cyber Safety Agreement and Authorisation Privacy and Confidentiality Procedure Safe use of Digital Technologies and Online Environments Policy

Sources

- Australian Children's Education & Care Quality Authority. (2025). *Guide to the National Quality Framework*
- Australian Children's Education & Care Quality Authority. (2023). *Embedding the National Child Safe Principles*
- Australian Children's Education & Care Quality Authority. (2024). *Taking Images and Video of Children While Providing Early Childhood Education and Care. Guidelines For The National Model Code*.
- Australian Government eSafety Commission (2020) www.esafety.gov.au
- Australian Government Department of Education. *Child Care Provider Handbook (2025)*
- Australian Government. eSafety Commissioner Early Years program for educators
- Australian Government, Office of the Australian Information Commissioner. (2019). Australian Privacy Principles: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/
- Australian Government Department of Health and Aged Care. (2021). Australia's Physical Activity and Sedentary Behaviour Guidelines
- Australian Human Rights Commission (2020). *Child Safe Organisations.* https://childsafe.humanrights.gov.au/
- Australia's Physical Activity and Sedentary Behaviour Guidelines
- Early Childhood Australia Code of Ethics. (2016).
- Education and Care Services National Law Act 2010. (Amended 2023).
- Education and Care Services National Regulations. (Amended 2023).
- NQF Online Safety Guide_1.pdf
- *Office of the Australian Information Commissioner (OAIC)*
- *Privacy Act 1988.*

Record of services' compliance (Reg 167)

Date Created: August 2025

Date Reviewed by Fun 4 U: 05/08/2025

Childcare Centre Desktop Policy Update: July 2025

This Policy Follows ACEQA: Child Safety | ACECQA, Digital technology and children | ACECQA & Chapter 2: Using digital technologies safely | ACECQA