Outside of School Hours Care

Policy

Safe Use of Digital Technologies and Online Environments

Purpose Statement

Children's safety and wellbeing is paramount, and Windermere's Out of School Hours Care (OSHC) Service has the responsibility to provide and maintain a safe and secure working and learning environment for staff, children, visitors and contractors, including online environments. We aim to create and maintain a positive digital safe culture that works in conjunction with our Service philosophy, and privacy and legislative requirements to ensure the safety of enrolled children, educators and families.

Windermere's OSHC Service is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and community. As a child safe organisation, OSHC embeds the National Principles for Child Safe Organisations (National Principles for Child Safe Organisations) and continuously addresses risks to ensure children are safe in physical and online environments. Digital technologies have become an integral part of many children's daily lives. For this reason, it is important that our educators are not only familiar with the use of digital technologies, but are able to guide children's understanding of, and ability to interact, engage, access and use a range of digital technology in a child safe environment.

Scope

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

Definitions

Refer to Appendix.

National Quality Standard (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2.3.	Child Safety and Protection (effective Jan 2026) abuse or neglect.	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 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		
168(ha)	The safe use of digital technologies and online environments at the service	

Safe Use of Digital Technologies and Online Environments

Policy Statement

TO MAINTAIN CHILDREN'S SAFETY AND RIGHT TO PRIVACY, ALL DEVICES USED FOR FAMILY DAY CARE MUST FIRST BE APPROVED BY THE COORDINATION UNIT.

Procedures

Implementation

Windermere's OSHC Service uses digital technology and electronic devices as a tool for learning with children, documenting their learning and development, communicating with families and the wider community, supporting program planning and administration tasks and enhancing safety and security through systems such as sign in/out platforms and CCTV monitoring. Our educators are diligent in ensuring children are only able to access age-appropriate technology.

Digital Technology and Electronic Devices Used at the Service

Windermere's OSHC Service adheres to the National Model Code for taking images or videos of children.

1. The approved provider will inform staff, educators, visitors, volunteers and family members that the use of personal electronic devices used to take photos, record audio or capture videos of children who are being educated and cared for at OSHC is strictly prohibited. This includes items such as tablets, phones, digital cameras, smart watches, META sunglasses and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage) and other new and emerging technologies. These devices should not be in the possession of staff, educators or visitors while working directly with children.
2. Staff and educators are advised that electronic devices issued by and registered with OSHC must not be removed from the premises as they may contain personal details of staff or children, including photos or videos. Exemptions may apply when required for operational activities, for example excursions or transportation.
3. The approved provider will inform staff, educators and visitors of exemptions that may warrant a person to use or be in possession of a personal electronic device that can be used to take images or videos. Staff, educators or visitors with an exemption must not use the personal device to take images or videos of children. Exemptions need to be provided for in writing by the approved provider and may include:
   - Emergency communication during incidents such as a lost child, injury, lockdown, or evacuation
   - Personal health needs requiring device use (e.g. heart or blood sugar monitoring)
   - Disability related communication needs
   - Urgent family matters (e.g. critically ill or dying family member)
   - Local emergency event to receive alerts (e.g. government bushfire or evacuation notifications).
4. Windermere's OSHC Service will develop and maintain a register of all electronic devices purchased for and used within the program. Each device purchased for and used at OSHC will be clearly marked with an identification code. This register will include details such as the identification code, device type, date of purchase, intended use, assigned user (if applicable). Devices recorded in the register may include, but are not limited to, computers, tablets, mobile phones, cameras, CCTV systems, audio recorders, smart toys, baby monitors and any other internet-connected or data-enabled devices used within the Service. Electronic devices issued by and registered with OSHC **will be stored in a locked cabinet at the end of the day**.

Images and Videos

1. The approved provider is responsible for determining who is authorised to take, use, store and destroy images and videos of children (using Service issued digital devices).
2. Images and videos will be stored securely with password protection, with access limited to authorised personnel only.
3. Images and videos of children must only be taken and used in accordance with OSHC policies, and careful consideration given to the purpose of the image or video.
4. Educators will engage in discussions that consider the intent, appropriateness, context and consent involved in capturing and using the images and videos, ensuring the process aligns with children's learning, wellbeing and right to privacy.
5. Windermere's OSHC will regularly review how digital data, including images and videos of children, is stored.
6. Digital data stored at OSHC will be destroyed in accordance with the *Record Keeping Policy*.
7. The approved provider will ensure staff, educators, visitors and volunteers do not transfer images or videos from Service issued devices to personal devices. Unauthorised transferring of digital data may result in disciplinary action.

Physical Environment and Active Supervision

The approved provider, nominated supervisor, management and educators will:

a. Ensure children are always supervised and never left unattended whilst an electronic device is connected to the internet

b. Provide a child safe environment to children- reminding them if they encounter anything unexpected that makes them feel uncomfortable, scared or upset, they can seek support from staff.

c. Reflect on OSHC's physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology:

   i. Perform regular audits to identify risks to children's safety and changes in room set-ups that can indicate areas of higher-risk and become supervision 'blind spots'.

   ii. Ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members when working with children

   iii. Only permit children to use devices in open areas where educators can monitor children's use

   iv. Be aware of high-risk behaviours for children online, including uploading private information or images, engaging with inappropriate content (inadvertently or purposefully), making in-app purchases, and interacting with unsafe individuals

   v. Ensure all visitors and volunteers are supervised at all times

d. Ensure all devices are password protected with access for staff only. Where digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure.

Software Programs and Apps

1. Windermere's OSHC Service uses a range of secure software programs and apps on Service-issued devices to support the educational program and its administration. All applicaitons used by staff, educators, visitors and children are carefully selected, regularly checked and kept up to date with the latest available system updates.

2. All applications installed on service issued devices undergo a request and assessment by Windermere's Information Technology team. Educators are unable to download any applications onto a service issued device due to Windermere security settings.

3. Access to software programs and apps are password protected to ensure the privacy of children, families and staff. Each user is provided their own user account and ensure log in, and password information is not shared.

4. The approved provider will ensure programs which require additional background checks, such as CCS Software, are only accessed by authorised staff who have completed necessary screening processes in accordance with Family Assistance Law.

5. Our educational program software is used by educators to share observations, photos, videos, daily reports, and learning portfolios with families in a secure, closed platform. In addition, Windermere's OSHC may use accounting and payroll software systems, and compliance tools that have been risk assessed by Windermere's IT team. These platforms assist in managing OSHC's financial, staffing, and operational requirements.

Confidentiality and Privacy Guidelines

1. Our *Privacy and Confidentiality Policy* applies to all use of digital technology and online environments. All staff, educators, and visitors must ensure that any information, images, or digital content related to children, families, and the OSHC Service is collected, stored, used, and shared in accordance with privacy legislation and service specific procedures, to maintain confidentiality and protect the safety and wellbeing of children.
2. Potential threats to security of information, unauthorised access to information (privacy breach) and loss of devices must be **reported at the time of the incident** by the educator to their nominated supervisor. Some examples of reportable incidents include:
    a. A device containing personal information about children and/or families is lost or stolen (parent names and phone numbers, dates of birth, allergies, parent phone numbers).
    b. A database with personal information about children and/or families is hacked.
    c. Personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report).
3. The nominated supervisor is to notify the approved provider **within 24 hours** of incidents related to point 2 above by emailing ohs@windermere.org.au and privacy@windermere.org.au.
4. Where an incident is assessed as being a notifiable data breach as defined by the Office of the Australian Information Commissioner (OAIC), the Privacy & Information Sharing Officer and Manager OSHC will submit an online report.

Identification and Reporting of Online Abuse and Safety Concerns

1. Windermere's OSHC Service will implement measures to keep children safe whilst using digital technology and accessing online environments.

2. The approved provider, nominated supervisor and management will:
   a. Ensure all staff, educators, students and volunteers are aware of their mandatory reporting obligations and promptly report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor.
   b. Support educators to:
      I. Encourage children to seek support if they encounter anything unexpected that makes them feel uncomfortable, scared or upset
      II. Listen sensitively and respond appropriately to any disclosures children may make relating to unsafe online interactions or exposure to inappropriate content.
      III. Respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management.
   c. Ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required.
   d. Report any suspected cases of online abuse to the relevant authorities, including the e-Safety Commissioner and Police, in accordance with legal requirements and child protection procedures.
   e. Notify the regulatory authority within 24 hours, via NQAITS, if a child is involved in a serious incident including any unsafe online interactions, exposure to inappropriate content, or suspected online abuse.

3. The Royal Commission recommends that organisations engaged in child related work retain records relating to child sexual abuse that has, or is alleged to have occurred, for at least 45 years (Royal Commission into Institutional Responses to Child Sexual Abuse, 2017).

Responsibilities

Windermere Responsibilities

The Approved Provider/Nominated Supervisor/Management will ensure:

- That obligations under the *Education and Care Services National Law and National Regulations* are met
- Educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure.
- New employees, students and volunteers are provided with a copy of the Safe Use of Digital Technologies and Online Environments Policy and procedure as part of their induction and are advised on how and where the policy can be accessed.
- All staff, educators, volunteers and students are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children.
- Families are aware of this Safe Use of Digital Technologies and Online Environments Policy and procedure and are advised on how and where the policy can be accessed.

- Processes are in place to ensure families who speak languages other than English understand the requirements of this policy, including providing authorisation for images and videos
- They promote and support a child safe environment, ensuring adherence to the *Child Safe Environment* and *Child Protection Policies*, including mandatory reporting obligations.
- The National Principles for Child Safe Organisations is embedded into the organisational structure and operations
- Professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments.
- Develop and monitor an *Electronic Device Register* for all electronic devices purchased and used at OSHC.
- Appropriate ratios and adequate supervision are maintained for children at all times including when using digital technology and accessing online environments.
- Students, volunteers and/or visitors are never left alone with a child whilst accessing OSHC Services.
- All staff, educators, volunteers and students are aware of the National Model Code and Guidelines (National Model Code – Taking images in early childhood education and care | ACECQA) and strictly adhere to these guidelines for taking images or video of children including but not limited to:
  - Personal electronic devices or personal storage devices, that can take images or videos, are not used by educators, staff, visitors or volunteers when working directly with children.
  - Staff and educators only use electronic devices issued and registered with the service for taking images or videos of children enrolled.
  - Service issued devices are securely configured, monitored and maintained to prevent unauthorised access.
- Written authorisation is obtained from parents/guardians for children to use electronic devices.
- Written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (website, Facebook, Instagram or hubworks).
- That OSHC seeks written authorisation from parents/guardians for their child to be photographed when used for marketing purposes or to take individual and group photos. Only children who have written authorisation from their parent/guardian will be included in any photography.
- Families are informed to withdraw authorisation, a written request is required
- Images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian.
- They review how images and videos are stored on a regular basis and ensure new educators and staff have access to relevant folders and files, if required, in accordance with their role.
- Digital data is stored securely, whether offline or online, and that data is archived regularly
- Images and videos are deleted or destroyed and removed from storage devices in accordance with the record keeping and retention policy, images and videos used for documenting children's learning and development must be held for 3 years after the child's last day of attendance.

- Every child in our care is protected from any exploitation of photographic and video images of themselves whilst in attendance.
- Images or videos of children must be appropriate in nature and must not show children in distress, in a position that may be perceived as sexualised or in a state of undress, including where genitalia may be exposed.
- External agencies or specialists are consulted if concerns are identified relating to online abuse, cyberbullying or digital safety risks.
- Policies and procedures reflect a commitment to equity and diversity, protect children's privacy, and empower children to be independent.
- Collaboration with relevant professionals, as required, to support equitable access to digital technologies for all children
- They remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the office of the Australian information commissioner (OAIC).
- A risk assessment is conducted regarding the use of digital technologies by staff and children at OSHC, including accessing online environments.
- Risk assessments for digital technology and online environments are reviewed annually or as soon as possible after becoming aware of any circumstances that may affect the safety, health or wellbeing of children.
- Policies and procedures are reviewed following an identification of risks following the review of risk assessments relating to the use of digital technologies and online environments.
- Staff, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies and online environments.
- A review of practices is conducted following an incident involving digital technologies or online environments, including an assessment of areas for improvement
- To install and maintain anti-virus and internet security systems including firewalls to block access to unsuitable web sites, newsgroups and chat rooms
- Educators are informed of, and adhere to recommended timeframes for 'screen time' according to Australia's physical activity and sedentary behaviour guidelines:
    - Children birth to one year should not spend any time in front of a screen
    - Children 2 to 5 years of age should be limited to less than one hour per day
    - Children 5-12 years of age should limit screen time for entertainment to no more than 2 hours a day.
- The use of TV/iPad and watching DVD's is kept to a minimum, with programs are chosen that are engaging and age appropriate to children. When used, the following conditions apply:
    - Only 'G' rated television programs and movies will be viewed at OSHC.
    - Programs depicting violence and/or inappropriate content (including graphic news reports) will not be shown
    - TV programs or videos will only be shown that have positive messages about relationships, family and life

  - Information about programs to be viewed will be shared with families beforehand to ensure that they approve of the content. Information may include title, synopsis, rating, length of program
  - All content will be socially and culturally considerate and appropriate.
- They share information to families about recommended screen time limits based on Australia's Physical Activity and Sedentary Behaviour Guidelines.
- All documentation and records relating to safe use of digital technologies are kept safe and secure for a period of 3 years following the child's last day of attendance.
- A review of practices is conducted following an incident involving digital technologies and online environments, including an assessment of areas for improvement.

- They share information to families about recommended screen time limits based on Australia's Physical Activity and Sedentary Behaviour Guidelines.
- All documentation and records relating to safe use of digital technologies are kept safe and secure for a period of 3 years following the child's last day of attendance.
- A review of practices is conducted following an incident involving digital technologies and online environments, including an assessment of areas for improvement.

OSHC Educator Responsibilities

OSHC Educators will:

- Adhere to the Safe Use of Digital Technologies and Online Environments Policy and associated procedure.
- Ensure they are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- Ensure they promote and support a child safe environment, including adherence to the Child Safe Environment and Child Protection policies and mandatory reporting obligations.
- Participate in practical training related to digital safety, privacy protection and responsible use of technology.
- Understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe.
- Promote and contribute to a culture of child safety and wellbeing in all aspects of OSHC's operations, including when accessing digital technologies and online learning environments.
- Not use, or have access to, any personal electronic devices, including mobile phones or smart watches used to take images or video of children.
- Not access social media (facebook, instagram or other) while working directly with children.
- Not breach children and families' privacy.
- Keep passwords confidential and log out of computers and software programs after each use.
- Ask permission before taking photos of children on any device and explain to children how photos of them will be used and where they may be published.

- Ensure children's personal information where children can be identified such as name, address, age, date of birth etc. Is not shared online.
- Ensure that screen time is not used as a reward or to manage challenging behaviours under any circumstances.
- Introduce concepts to children about online safety at age-appropriate levels.
- Support children's understanding of online safety by providing age-appropriate guidance, discussions and activities that help them to recognise safe and unsafe online behaviours.
- Consult with children about matters that impact them, including the use of digital technologies and online environments, to ensure their voices are heard and respected in a meaningful way.

Family Responsibilities

Families will:

- 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 OSHC.
- Provide written authorisation indicating whether or not OSHC may take, use, store or destroy images or videos of their child.
- Provide written notification if they wish to withdraw the authorisation for OSHC to take, use, store or destroy images and videos of their child.
- Be able to withdraw authorisation for OSHC to take, use, store or destroy images or videos of children at any time in writing.
- Be provided with clear information about how to make a complaint and our complaints handling processes.
- Be aware that sometimes other children in the OSHC Service may feature in the same photos, videos, and/or observations as their children. In these cases, families are never to duplicate or upload them to the internet/social networking sites or share them with anyone other than family members.

Visitor and Volunteer Responsibilities

Visitors and Volunteers will:

- Adhere to the Safe Use of Digital Technologies and Online Environments Policy and associated procedure whilst visiting OSHC.
- 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 OSHC.
- Report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor.

Breach of Policy

1. Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment and may face disciplinary action which may lead to notification to the regulatory authority and child protection authorities.
2. Visitors or volunteers who fail to comply to this policy may face termination of their engagement.
3. Family members who do not comply with this policy may place their child's enrolment at risk and limit the family members' access to the OSHC Service.

Relevant Legislation/ Standards

- National Quality Framework for Early Childhood Education and Care Services including:
  - Education and Care Services National Law 2011 (Amended 2024)
  - Education and Care Services National Regulations 2011 (Amended 2024)
- Child Care Subsidy Secretary's Rules 2017
- Family Law Act 1975
- A New Tax System (Family Assistance) Act 1999
- Privacy Act 1988 (the Act)
- The National Mode Code (2024)
- Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook (Child Care Provider Handbook)

Related Policies & Links

- Australian Children's Education & Care Quality Authority. (2024). Guide to the National Quality Framework.

Safe Use of Digital Technologies and Online Environments

DEFINITIONS	
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.
Cyberbullying	When someone uses the internet to be mean to a child or young person so they feel bad or upset.
Cyber safety	Safe and responsible use of the internet and equipment/devices, including mobile phones and devices.
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.
Generative artificial intelligence (AI)	A branch of AI that develops generative models with the capability of learning to generate novel content such as images, text and other media with similar properties as their training data.
Harmful content	Harmful content includes sexually explicit material; false or misleading information; violence; extremism or terrorism; hateful or offensive material
ICT	Information and Communication Technologies.
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 Footage of real violence, cruelty and criminal activity
Optical Surveillance Device	Has the same meaning as in section 6(1) of the Surveillance Devices Act 2004 of the Commonwealth
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender
Smart toys	Smart toys generally require an internet connection to operate as the computing task is on a central server
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
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed