Intereach Outside of School Hours

Safe use of Digital Technologies and Online Environments Procedure

Applies to	Intereach Outside of School Hours care (OOSH)				
Policy	NQS Two – Children's Health and Safety Policy				
Version	1.0	**Date approved**	02/09/2025	**Next review date**	02/09/2028

1. Objective

Intereach as the approved provider is committed to create an environment where children are not only physically safe but also digitally secure while ensuring their safety, health and wellbeing.

This procedure aims to ensure that all digital interactions within the service are safe, age-appropriate, and comply with relevant legislation and best practices. It supports educators, staff, and families in fostering a secure digital environment that promotes responsible use of technology and protects sensitive information.

2. Background

In an increasingly digital world, online and digital technologies are becoming essential tools in Early Childhood Education and Care (ECEC) environments for learning, communication, and administration. While these technologies offer significant benefits, they also present potential risks to the safety, privacy, and wellbeing of children, families, and educators. Young children are particularly vulnerable due to their limited understanding of online safety and the long-term impact of digital exposure.

Under the Education and Care Services National Regulation 168, 169 and 170 and the National Principles for Child Safe Organisation Principle 8 Children are safe online; an approved provider must ensure that policies and procedures are in place for the safe use of digital technologies and online environments at the service. which guides the safe use of digital devices, protect children's personal information and digital identities, and ensure all online practices reflect a child-safe culture.

3. Responsibilities

It is the responsibility of the Nominated Supervisors and Coordination Unit staff to:

- ensure that obligations under the Education and Care Services National Law and National Regulations are met;
- take reasonable steps to ensure all staff and educators follow the safe use of digital technologies and online environments procedure;
- take reasonable steps to ensure the safe use of digital technologies, including smart watches, smart toys, and online environments at the service;
- take reasonable steps to ensure that any digital technologies, including smart watches, smart toys etc that are in possession of a child are stored securely whilst child is in the service.
- train staff in safe digital practices and ensure they are aware of the Child Safe Standards in relation to online safety;
- ensure staff understand how to actively supervise children while using digital technologies;

- support staff to uphold the service's culture of child safety and wellbeing; including when accessing digital technologies and online learning environments
- provide resources and opportunities for ongoing training;
- have ongoing communication with staff about their responsibilities and any changes to policies, procedures and legislation, particularly as digital technologies evolve quickly;
- communicate and provide information and resources to families on safe use of digital technologies and online environments;
- only used service issued devices when capturing images or videos of children enrolled at OOSH for the purposes of documentation; and,
- have a register for service issued devices.

It is the responsibility of Staff to:

- implement the safe use of digital technologies and online environments policy and procedures;
- participate in eSafety Training: e Safety Professional Learning Modules - ECA and the eSafety Commissioner (earlychildhoodaustralia.org.au), and to ensure up to date knowledge in safe practice;
- have programs in place to educate children to be promoting safe, responsible and discerning in the use of digital technologies; for example, but not limited to, resources accessed via e-safety Commissioner website https://www.esafety.gov.au/educators/classroom-resources
- ensure use of online sites and digital technologies are learning centred;
- ensure a risk assessment is carried out for using electronic devices,
- ensure active supervision of children when they are using digital technologies;
- understand and monitor for signs of online grooming or inappropriate contact through messaging, chat functions, or game platforms;
- facilitate age-appropriate conversations that empower children to make safe decisions online and express their preferences regarding the use of technology;
- understand the National Model Code and the service's expectations around the use of personal devices while at the service, and seek guidance when needed from the Nominated Supervisor and/or Team Leader;
- communicate with families that personal devices are banned at the service unless for essential purposes;
- recognise and respond effectively to children and young people when discussing the use of digital technologies and online environments, considering diverse needs and interests;
- Implement strict storage controls for children's digital data. Consider the security of the digital data and the privacy of children and families when using digital platforms,
- ensure children and young people participate in decision-making in matters affecting them regarding the safe use of digital technologies and online environments at the service;
- ensure all media consent arrangements are adhered to;
- have regular conversations with families regarding consent and ensure annual update of child enrolment forms that includes consent;
- ensure visitors, contractors, students and volunteers refrain from using their personal devices around children;
- provide information and resources to families on safe use of digital technologies and online environments;
- Not share group photos where children are identifiable

It is the responsibility of Parents/Guardians to:

- read and understand the OOSH Safe Use of Digital Technologies and Online Environments Procedure;
- engage in opportunities for digital literacy education offered by the service;
- ensure media consent is up to date;
- support digital safety practices;
- understand that if children have digital devices in their possession when arriving at our OOSH services these must be presented to staff to store securely until child is collected from service,
- not take images or videos of children within the education and care service or at events such as regular outings and excursions
- Talk to and educate children in relation to our service procedure and their responsibility to comply

4. Procedure

All children attending the service are provided with a safe environment through the creation and maintenance of a child safe culture, and this extends to the safe use of digital technologies and online environment.

4.1. Conducting Detailed Assessment

Staff must adhere to strict controls in place for the appropriate storage and retention of images and videos of children. Appropriate risk assessments and action plans are completed, and all identified actions are taken to minimise the risks to children's health and safety and to promote a culture of child safety and wellbeing that underpins all aspects of the service's operations (including online learning environments), to reduce risk to children (including the risk of abuse).

Staff identify and mitigate risks in the online and physical environments without compromising a child's right to privacy, access to information, social connections and learning opportunities (refer to Child Safety Standard Vic 9.1 and NSW 8).

4.2. Management of images and videos of children: Capture, use, storage and disposal

It is important to safeguard children's privacy and dignity in all digital practices and comply with the relevant legislation, child protection standards and the National principles for Child Safe Organisations when capturing, using, storing, and securely disposing of images and videos of children.

4.2.1. Capturing images

Staff may use personal digital devices (such as smartphones or tablets) for work-related purposes including programming, communication, or capturing images of children, only when:

- written consent has been obtained from parents/guardians for any images or videos.

Inappropriate images or videos are strictly prohibited from being taken, inappropriate images or videos are any that are not relevant to the child's learning and development, examples include:

- where a child is not appropriately dressed, i.e. in their underwear;
- in a position that could be perceived as sexualised in nature; and,
- in a distressed or anxious state;

Visitors, contractors, students and volunteers are strictly prohibited from using their personal devices to take photos, videos, or access digital content related to children in care.

Any child support services that visit the service are only permitted to use business/employer issued devices (i.e. laptops and tablets) where it is required to perform their professional functions (i.e. taking notes/observations, filling in forms, part of a child's therapeutic treatment such as speech therapy applications etc.) where it would impede their ability to carry out their professional function without it. No photos are to be taken unless parent authorisation is sought.

4.2.2. Use of Digital Technology

The service may utilise secure online platforms (e.g., Harmony, Authorised Educational Programming Apps) to share updates and communicate with families and the broader community. When engaging in such communication, the service will ensure that:

- all content shared respects the privacy and dignity of children and families;
- appropriate consent has been obtained prior to sharing any images, videos, or personal information;
- platforms are used in accordance with the service's digital safety and child protection policies and procedures;
- communication remains professional, respectful, and aligned with the service's values and educational objectives;
- online platforms are password protected and use multifactor authentication;
- understand where and how information is stored and the terms and conditions of the online platforms being used;
- avoid identifying images of children where possible; and,
- all social media posts are professionally composed and accompanied by appropriate, consented photographs that reflect the values and standards of the service.

When images are taken for the purpose of social media, parent consents are in place, and images are shared securely with our Communications and Marketing teams who will adhere to security and privacy obligations before posting.

- Staff will not share images or videos of OOSH children on any personal platforms under any circumstances.
- Staff must not share images or videos of children for social media purposes who:
    - are/have been subject to child protection, family court or criminal proceeding, or other legal matters where their identity must be protected (following legal instructions).
    - are experiencing family violence and need to stay anonymous
    - have parents who are concerned about their child's digital footprint and request limited or no online photos.

4.3. Storage of Digital documents or photos

- Where photos of children are stored, the device must be password-protected and regular security updates are completed.
- Where folders can be created with additional passwords, this practice is recommended.

- Under regulation 183, the NQF requires all records relating to a child enrolled at the service to be kept for 3 years from the last day they were educated and cared for by the service, unless the record:
    - relates to an incident, illness, injury or trauma suffered by a child while being educated and cared for by the service or may have occurred following an incident whilst being educated and cared for by the service, in which case the record must be kept until the child is age 25, or
    - is in relation to the death of a child while being educated and cared for by the service, in which case the record must be kept until 7 years after the death.
    - Relates to child sexual abuse which should be retained for at least 45 years as recommended by the Royal Commission
- All images and videos must be deleted once they have served their intended purpose. For example, images of children should not be retained on personal devices for personal keepsakes or mementos by educators.

4.4. Disposal of electronic documents

All electronic data must be kept for the timeframes stated above under 4.2.and then destroyed properly.

- Australian Privacy Principles 11.1 and 11.2 require personal information to be protected then destroyed or de-identified when it's no longer needed. Make sure electronic records are completely removed, not just deleted.

4.5. Use of Artificial Intelligence (AI)

Intereach OOSH staff, may engage the use of Artificial Intelligence tools. AI can complement an educator's skills, however, must always be used in a manner that priorities the safety and wellbeing of children.

- Never share personal information about children or others when using AI tools. For example, if using an AI tool to summarise a child's learning experiences, always remove any identifying details before entering them into the tool. Use random initials and birthdates.
- Do not include images or videos into AI tools.
- Any content created by AI will be checked by an educator to make sure it is accurate and appropriate.
- Assume any information being input into generative AI tools could become public and think about what is appropriate to include.
- Communicate to families that AI is being used.
- Only used paid and verified AI tools to ensure the highest standards of data protection and privacy such as Copilot.

4.6. Authorisation for sharing digital content

Parental/guardian consent is required before capturing or sharing any digital content involving children. Parents have the right to withdraw consent at any time.

Permission will be sought from children before taking their image or video and explained how the image or video will be used in age-appropriate ways with their responses respected. Children will not be forced or manipulated into having their photo taken.

4.7. Use of Optical Surveillance (E.g. CCTV)

Surveillance equipment is permitted to be installed however must be positioned to respect privacy

The Families must be informed about the surveillance and where it is located if surveillance records people:

- individuals, must be informed before they're recorded, that their personal information may be captured,
- clear signage, that is easy to understand, must be available to indicate the presence of surveillance equipment; and,
- ensure only authorised people have access to recorded data, these people include educators, service staff and department of education staff and where necessary police.

Cameras and devices connected to the internet can be hacked, so it's important to keep them secure. For example, the connection of webcams to wireless networks adds extra privacy risks because of the increased possibility of data being intercepted by people using electronic hacking devices.

4.8. The use of digital devices by children

Educators will ensure active supervision of children when using devices.

- Check privacy settings and age restrictions regularly.
- Check the risks of smart toys and, where possible, disconnect them from the internet to avoid hacking.
- Turn off chat functions on apps and games.
- Choose app settings that turn off location sharing and enable privacy controls.
- Children will be supported to develop age-appropriate understanding of:
    - Online safety and respectful technology use.
    - How to seek help if they feel unsafe or unsure online.
- Children will have a voice in decisions involving their digital presence.
- Use the eSafety Commissioner's play-based resources to explore digital concepts like protecting personal information, respectful relationships and being a good digital citizen.
- Communicate with children and families about online risks (in an age and developmentally appropriate way), using conversation starters from the eSafety Commissioner: For example "Talking about child sexual abuse online with 4 to 12-year-olds". Inform families about how the service communicates with children about these issues, ahead of time, to build a shared understanding of child safety.
- Children will not be permitted to use personal devices including iPads, laptops, smart watches and smart toys from home (or school issued) when attending OOSH. Devices are stored securely until collection of child at the end of service

4.9. Use of screen time

The Australian Department of Health provides research-based recommendations for physical activity, sedentary behaviour, and sleep for children and young people. Staff are encouraged to implement these guidelines in their daily practice, including the following: Across a 24-hour period, it is recommended:

- Children up to age of 5 have no more than one hour of screen time per day; and,
- children and young people aged between 5-17 years have less than 2 hours a day of sedentary recreational screen time.

These time limits do not include the screen time spent on educational activities. (Refer to *Physical activity and Small Screen Time Procedure*).

Visit the Australian Department of Health's Physical Activity and Sedentary Behaviour Guidelines

4.10. Engaging family

Families will be informed about the service's digital safety procedures, including:

- platforms and tools in use at OOSH;
- their child's access to digital devices (if any); and,
- how media consent is managed and upheld.

Families are encouraged to raise any concerns or questions about digital safety practices.

4.11. Responsible use of technology

The use of Television, watching DVD's, streaming educational programs, accessing online based educational games and online research activities will be kept to a minimum. (Refer to *Physical Activity and Screen Time Procedure*).

- Programs/games depicting violence and/or inappropriate content (including graphic news reports) will not be shown.
- TV programs, DVD or streamed programs will only be shown that have positive educational messages about relationships, family and life and must be classified G (General) under the Australian Classification rating. PG programs will require parent consent before implementation.
- Information about programs to be viewed will be shared with families beforehand to ensure that they approve of the content.
- All content will be socially and culturally considerate and appropriate.

4.12. Reporting concerns or breaches

All breaches or concerns about digital or online safety must be reported to the Nominated Supervisor or Team Leader immediately.

If child safety is compromised, appropriate child protection procedures will be followed.

All incidents will be recorded, reviewed, and addressed in a timely manner.

4.13. Responding to online incidents

Responding to online incidents effectively is crucial to minimize harm and ensure safety. Refer to the quick reference guide for responding to online safety incidents. Refer to Quick Reference guide for responding to online safety incident (eSafety.gov.au) for steps to follow when an incident is identified.

If an incident occurs, staff will:

- take action immediately - If the incident involves a device staff will disconnect the device and report it as an incident;
- determine the nature and the scope of the incident and evaluate impacts to service;
- take steps to contain such incident and to prevent it from happening again; and,
- communicate the incident and the actions taken to families and other relevant parties (Refer to *Intereach Risk Management Policy, Incident Management Policy* and *Incident, Injury, Trauma and Illness Procedure)*

4.14. Evaluating measures

The incidents, complaints and feedback from children and families will be tracked for evaluating purposes and assessing staff confidence and training uptake annually.

Children's voices will be gathered through age-appropriate methods (e.g., drawings, discussions, storytelling) to shape digital learning environments.

5. Monitoring, evaluation and review

This procedure will be reviewed every three years and incorporate feedback and suggestions from children, families, staff, volunteers, and students.

6. National Quality Framework

Element	Concept	Description
2.1.2	Health practices and procedures	Effective illness and injury management and hygiene practices are promoted and implemented.
2.2.1	Supervision	At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard
2.2.2	Incident and emergency management	Plans to effectively manage incidents and emergencies are developed in consultation with relevant authorities, practiced and implemented
2.2.3	Child Safety and protection	Management, 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
3.1.1	Fit for purpose	Outdoor and indoor spaces, buildings, fixtures and fittings are suitable for their purpose, including supporting the access of every child.
3.1.2	Upkeep	Premises, furniture and equipment are safe, clean and well maintained.
3.2.1	Inclusive environment	Outdoor and indoor spaces are organised and adapted to support every child's participation and to engage every child in quality experiences in both built and natural environments.
4.1.1	Organisation of educators	The organisation of educators across the service supports children's learning and development.
7.1.1	Service philosophy and purpose	A statement of philosophy guides all aspects of the service's operations.
7.1.2	Management Systems	Systems are in place to manage risk and enable the effective management and operation of a quality service that is child safe.
7.1.3	Roles and responsibilities	Roles and responsibilities are clearly defined, and understood, and support effective decision making and operation of the service.
7.2.1	Continuous improvement	There is an effective self-assessment and quality improvement process in place.

Element	Concept	Description
7.2.3	Development of professionals	Educators, and staff members' performance is regularly evaluated, and individual plans are in place to support learning and development.

7. **Context**	
3.1 Standards or other external requirements	Australian Privacy Principles Information Privacy Principles (Vic) National Model Code National Quality Standards Child Safe Standards NSW Child Safe Standards VIC
3.1 Legislation or other requirements	Relevant legislation and standards include but are not limited to: Education and Care Services National Law Act 2010 Education and Care Services National Regulations 2011 Early Childhood Australia Code of Ethics National Quality Standard, Quality Area 2: Children Health and Safety and Quality Area 7: Governance and Leadership National Principals of Child Safe Organisations – Principal 8 national-principles-for-child-safe-organisations.PDF (childsafety.gov.au) Privacy Act 1988 (Cth) United Nations Convention on the Rights of the Child The most current amendments to listed legislation can be found at: Commonwealth Legislation – Federal Register of Legislation: www.legislation.gov.au

3.2 External Documents	Early Childhood Australia Statement on young children and digital technology: http://www.earlychildhoodaustralia.org.au/wp-content/uploads/2018/10/Digital-policy-statement.pdf My Time Our Place Frameworks for School Age Children: My Time Our Place Framework eSafety Commissioner: https://www.esafety.gov.au/ eSafety's professional learning modules: https://www.esafety.gov.au/educators/training-for-professionals/early-years Online Safety Agreement: https://www.esafety.gov.au/educators/early-years-program/online-safety-agreement The eSafety Guide: https://www.esafety.gov.au/key-issues/esafety-guide Child Safe Organisations - Checklist for Online Safety The Playing IT Safe Framework and Alignment: https://playingitsafe.org.au/ Approved Early Years Learning and Development Frameworks: https://www.acecqa.gov.au/nqf/national-law-regulations/approved-learning-framework BELONGING, BEING & BECOMING - THE EARLY YEARS LEARNING FRAMEWORK | ACECQA MY TIME, OUR PLACE - FRAMEWORK FOR SCHOOL AGE CARE IN AUSTRALIA | ACECQA
3.3 Internal documents	Intereach Privacy Policy Intereach Social Media Policy Intereach Data Security and Retention Policy Intereach Child Safe Policy Intereach Code of Conduct Policy Intereach Risk Management Policy Intereach Incident Management Policy Incident, Injury, Trauma and illness procedure Physical activity and screen time Procedure

4 Document control

Version	Date approved	Approved by	Next review date
1.0	2 September 2025	J Farrow - Manager Education and Care	2 September 2028