# Digital Technology and Online Environments Safety Policy

## NATIONAL QUALITY STANDARDS

This policy relates to:

**Quality Area 2: Children's Health and Safety**

- 2.2. – *Safety*: Each child is protected.
- 2.2.1- Supervision: At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.
- 2.2.3- Child Safety and Protection: Management, educators and staff are aware of their roles and responsibilities 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 systems*: Systems are in place to manage risk and enable the effective management and operation of a quality service that is child safe.

**STATEMENT**

Our Service is dedicated to creating and sustaining a safe online environment through the active involvement of staff, families, and the wider community. As a child safe organisation, we are committed to embedding the National Principles for Child Safe Organisations into our practices and continuously identifying and managing risks to ensure children's safety in both physical and digital spaces.

With digital technologies now playing a significant role in many children's lives, it is essential that our educators not only understand these technologies but also support children in developing safe, respectful, and informed digital habits within a child safe environment.

**RATIONALE**

The safety and wellbeing of children is our highest priority. Our Service is committed to providing and maintaining a secure and supportive environment for all staff, children, families, visitors, and contractors-both in physical and online settings.

We strive to foster a positive digital safety culture that aligns with our Service philosophy and complies with all relevant privacy and legislative requirements to protect the wellbeing of enrolled children, educators, and families.

**IMPLEMENTATION**

**Use of Digital Technologies at the Service**

Our Service integrates digital technology and electronic devices to enhance children's learning experiences, document development, communicate with families and the broader community, support curriculum planning and administrative functions, and strengthen safety measures such as sign-in/out systems. Educators ensure that children access only age-appropriate content using devices provided by the Service.

**Digital Devices and the National Model Code**

We align our practices with the National Model Code and Guidelines for the responsible use of images and videos of children. While implementation is currently optional, changes in legislation are anticipated that may enforce a ban on the use of personal digital devices in early childhood settings, with non-compliance potentially resulting in fines.

The approved provider will clearly inform all staff, educators, visitors, volunteers, and family members that the use of personal electronic devices-including mobile phones, tablets, smartwatches, META smart glasses, cameras, and data storage devices (USBs, SD cards, hard drives, and cloud services)- to capture images or recordings of children is strictly prohibited. These devices are not to be carried or used while working directly with children.

Devices belonging to the Service must remain onsite unless taken offsite for approved purposes such as excursions or transport. These devices may contain sensitive data related to children, families, or staff.

**Exemptions for Personal Devices**

In specific, approved circumstances, individuals may be permitted to carry a personal device, with written authorisation from the approved provider. However, these devices must not be used to photograph or record children. Approved exemptions may include:

- Emergency situations (e.g. child missing, lockdown, injury)
- Health requirements (e.g. glucose or heart rate monitoring)
- Communication support for a disability
- Urgent family communications (e.g. serious illness or death)
- Receipt of emergency alerts (e.g. bushfire notifications)

**Electronic Device Register**

A detailed register is maintained, listing all Service-purchased electronic devices. The register outlines the type of device, purchase date, intended use, assigned user (if applicable), security settings, and data capabilities. Devices may include computers, tablets, mobile phones, cameras, CCTV systems, baby monitors, audio recorders, and any connected or data-enabled devices.

**Children's Use of Devices**
Children are not permitted to bring personal electronic devices to the Service unless approved by the approved provider or nominated supervisor for a specific medical or developmental reason. Unapproved devices brought to the Service will be turned off and securely stored.

**Images and Videos**
Only authorised personnel may capture, use, store, or dispose of images and videos using Service-issued devices. These media files are password-protected and stored securely. Educators must consider the purpose, appropriateness, and consent when capturing digital content. Monthly reviews of storage practices are conducted, and backups are maintained. Deletion of content follows the Record Keeping and Retention Policy. Transferring images or videos to personal devices is prohibited and may result in disciplinary action.

**Supervision and the Physical Environment**
The approved provider and educators must:

- Maintain supervision whenever children use internet-connected devices
- Provide a safe and supportive digital environment
- Regularly audit the physical space to identify risks and ensure safe tech use
- Ensure digital equipment is visible and used only in monitored, open areas
- Prevent access to high-risk online behaviors such as sharing personal information, accessing inappropriate content, or unsafe communication
- Password-protect all devices with access restricted to staff
- Follow policy procedures during excursions and transport

**Software and Applications**
The Service uses secure, regularly updated software and apps on Service-owned devices for educational, administrative, and communication purposes. Access is protected with individual logins and passwords. Systems such as CCS software, MYOB, Xero, and HR platforms are accessible only by authorised personnel.

**Artificial Intelligence (AI) Use**
Staff using AI must acknowledge its limitations and privacy concerns. AI can be a supportive tool for documentation but must not replace professional judgement. Staff are only to use our centre-owned AI software (Childcare Tools) to aid in the development of documentation relating specifically to children, families, or groups in our service. Personal data (e.g. children's names or DOB) must not be entered into any other AI systems outside of Childcare Tools. All AI-generated information must be verified and tailored to the specific context.

**Privacy and Confidentiality**
All digital interactions must comply with the Service's Privacy and Confidentiality Policy and

relevant legislation. Staff and visitors must handle all digital content involving children or families responsibly. Any suspected breach must be reported immediately. In the event of a data breach, the OAIC will be notified using the Notifiable Data Breach Form. Examples include lost devices, misdirected reports, or hacking incidents.

**Identifying and Reporting Online Risks**

The Service implements safeguards to protect children online. Staff are trained in mandatory reporting and respond promptly to child safety concerns, including digital-related incidents. Reports are made to the eSafety Commissioner, Police, and regulatory bodies as required, and concerns are documented and addressed with family support.

**Approved Provider Responsibilities**

The approved provider ensures:

- Compliance with national laws and regulations
- Staff and volunteers understand and follow this policy
- Induction processes include the digital safety policy
- National Child Safe Principles are embedded in operations
- Ongoing professional learning in digital safety
- Electronic Device Register is monitored
- Active supervision and appropriate ratios are maintained
- Visitors and students are never left alone with children
- Staff use only Service-issued devices for images and videos
- Visitors get written consent to capture images (e.g. professional photographer, students)
- Complaints processes are accessible
- Images are managed with parental consent
- Screen time is managed per national guidelines
- Families are educated on safe screen use

**Educators Will:**

- Follow all digital safety policies and procedures
- Understand mandatory reporting and child safety obligations
- Participate in training on digital safety
- Actively supervise digital technology use
- Promote child safety and privacy
- Keep passwords confidential
- Educate children on online safety in age-appropriate ways

**Families Will:**

- Follow the digital safety policy
- Avoid capturing digital content of children while onsite
- Not share Service-related images of children on social media

**Visitors and Volunteers Will:**

- Comply with this policy during visits
- Avoid using personal digital devices to capture images
- Report any digital safety concerns
- Obtain written consent when necessary

**Policy Breaches**

Non-compliance may result in disciplinary action, removal from the premises, or review of a child's enrolment status depending on the role of the individual involved.

**Education and Care Services National Regulations 2011**

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 services must have policies and procedures

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

**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 Children's Education & Care Quality Authority. (2025). *NQF Online Safety Guide*

Australian Government eSafety Commission (2020) www.esafety.gov.au

Australian Government Department of Education.(2025). *Child Care Provider Handbook*

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/

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).

*Office of the Australian Information Commissioner (OAIC)*

*Privacy Act 1988.*

*Western Australian Legislation Education and Care Services National Law (WA) Act 2012*

*Western Australian Legislation Education and Care Services National Regulations (WA) Act 2012*


## RESOURCES

Australian Children's Education & Care Quality Authority. National Model for Early Childhood Education and Care.

Australian Government Office of the eSafety commission

eSafety Early Years Program for educators

eSafety Early Years Program checklist

eSmart Alannah & Madeline foundation

Family Tech Agreement. eSafety Early Years Online safety for under 5s

Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content: https://www.kiddle.co/

Office of the Australian Information Commissioner (OAIC)

**Policy Review**

- The Service will review this policy and guidelines every 12 months.
- Families are encouraged to collaborate with the service to review policies and procedures.
- Educators/Carers are essential stakeholders in the policy review process and are encouraged to be actively involved.

| | |
|---|---|
| Developed | August 2025 |
| Last Reviewed | |
| Next Review | August 2026 |