SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS POLICY

Our 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, our Service embeds the National Principles for Child Safe Organisations and Child Safe Standards and continuously addresses risks to ensure children are safe in physical and online environments.

NATIONAL QUALITY STANDARD (NQS)

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 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. 2A	Paramount consideration—safety, rights and best interests of children
S. 3A	Paramount consideration
S. 162A	Child protection training
S. 162B	Child safety training
S. 165	Offence to inadequately supervise children
S. 166A	Offence to subject child to inappropriate conduct Offence relating to inappropriate conduct
S. 167	Offence relating to protection of children from harm and hazards
S.174(2)(a)	Notification of serious incident
PART 6A	Devices in education and care services
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(2)(ha)	The safe use of digital technologies and 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
179A	Prescribed information to be kept in written record of authorisation to possess or control personal device
179B	Prescribed period to keep written record of authorisation to possess or control personal device
181	Confidentiality of records kept by approved provider
183	Storage of records and other documents
184	Storage of records after service approval transferred

RELATED LEGISLATION

Surveillance Devices Act 2004 (Cth)	*Privacy Act 1988* (Cth)

RELATED POLICIES

Child Safe Environment Policy Child Protection Policy Code of Conduct Policy Dealing with Complaints Policy Educational Program Policy Enrolment Policy Governance and Leadership Policy	Incident, Injury, Trauma, and Illness Policy Interactions with Children Families and Staff Policy Privacy and Confidentiality Policy Protected Disclosure (Whistleblower) Policy Record Keeping and Retention Policy Student, Volunteer and Visitor Policy Supervision Policy

PURPOSE

Children's safety and wellbeing is paramount, and our 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. We believe that children's safety, rights, and best interests are the paramount consideration for all Service operations, decisions and functions.

This policy provides the framework for:

- the safe use of digital technologies and electronic devices at the Service
- the capture, use, storage and destruction of images and videos of children whilst being educated and cared for by the Service
- obtaining written authorisation from parents to take, use and store images and videos of children
- the use of digital devices by children whilst being educated and cared for at the Service
- the responsible use of online environments, including artificial intelligence (AI) tools and software platforms

SCOPE

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

TERMINOLOGY	
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.
Capturing	An image includes filming, recording or taking a photo/image of a child
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.
Digital devices	All electronic equipment capable of capturing, storing, transmitting or receiving data, images or video- including computers, tablets, mobile phones, cameras, smart watches, wearable devices, baby monitors, smart toys and any other internet-connected data-enabled 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	Content that includes images and videos of child sexual abuse, content that includes terrorist acts, content that promotes, incites or instructs in crime or violence or footage of real violence, cruelty and criminal activity.

Images and videos of children	Any photographic, video or audio recording of children being education and cared for by the Service, whether captured on Service-supplied or personal devices
National Model Code	The National Model Code for Early Childhood Education and Care, released by ACECQA which provides guidelines about the use of personal electronic devices in education and care services, including taking images or video of children.
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender
Online environments	Any internet-connected platform, application, website or digital service accessed or used at or in connection with the Service
Personal electronic devices	A device that is owned by a person (NOT owned/supplied by an approved provider for education and care purposes) and is capable of capturing, storing or transmitting an image or video. Includes personal mobile phones, tablets, smart watches, META sunglass (wearables), personal cameras and personal storage media such as SD/memory cards, USB drives, hard drives and cloud storage and other new emerging technologies
Service-supplied devices	A device owned or supplied by an approved provider and is used exclusively to provide education and care. It may capture, store or transmit images and video of children. Examples include phones, cameras, tablet computers and hard drives.
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, using a phone service or any platform that allows online messaging or chat
Transmitting	Includes sharing a photo by text message, email, USB/hard drive, uploading to social media or information sharing platform or any other form of distributing an image or recording, including live streaming
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed

Source: Glossary to NQF Child Safe Culture and Online Safety Guides- ACECQA 2025 and ACECQA 2026 Using digital devices in centre-based education and care services

IMPLEMENTATION

Our Service uses digital technology and electronic devices to support children's learning and development, document educational programs, communicate with families and the wider community, and facilitate administration and safety systems including sign in/out platforms.

The use of digital technologies is guided by the paramount consideration of child safety and wellbeing. Our Service ensures that all digital environment, devices and online platforms are used in ways that protect children from harm, uphold privacy and confidentiality and prevent inappropriate conduct.

THE APPROVED PROVIDER/NOMINATED SUPERVISOR/MANAGEMENT RESPONSIBILITIES:

Governance and Compliance

- ensure that obligations under the Education and Care Services National Law (including Part 6A) Education and Care Services National Regulations and regulator directions are met
- ensure educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure
- take every reasonable precaution to prevent breaches of this policy and related legislation
- ensure families are aware of this policy and advised how and where it can be accessed

- ensure 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
- ensure mandatory national child safety training is completed by the approved provider, management, staff, educators, students and volunteers
- ensure child safe practices are embedded into organisational practice as per National Principles for Child Safe Organisations and Child Safe Standards
- remain informed of updates to privacy legislation and guidance from the Office of the Australian Information Commissioner (OAIC)
- ensure children, educators and families are aware of the Service's complaints handling process to raise any concerns they may have about the use of digital technologies or any other matter (see: *Dealing with Complaints Policy*)
- ensure staff, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies.

Induction, Training and Professional Learning

- ensure 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
- provide professional learning to educators and staff regarding the safe use of digital technologies and online environments.

Child Safety Culture

- 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 or inappropriate conduct to the approved provider or nominated supervisor [See *Child Protection Policy*]
- promote and support a child safe environment, ensuring adherence to the *Child Safe Environment and Child Protection Policies,* including mandatory reporting obligations
- maintain appropriate educator to child ratios and active supervision at all times, including when using technology
- ensure all students, visitors and volunteers are supervised at all times and never left alone with a child
- conduct risk assessments regarding the use of digital technologies by staff and children
- review risk assessments annually or as soon as practicable after becoming aware of circumstances that affect child safety
- ensure a review of practices is conducted following an incident involving digital technologies and online environments, including an assessment of areas for improvement
- ensure reasonable precautions are taken to prevent personal device use in breach of National Law and regulator directions
- install and maintain anti-virus and internet security systems including firewalls to block access to unsuitable websites, newsgroups and chat rooms
- support educators to:
    - encourage children to seek support if they encounter anything unexpected that makes them feel uncomfortable, scared or upset
    - listen sensitively and respond appropriately to any disclosures children may make relating to unsafe online interactions or exposure to inappropriate content, adhering to the *Child Protection Policy, Behaviour Guidance* and reporting procedures
    - respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management
- ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required
- ensure all educators, staff, students and families are advised of the *Protected Disclosure (Whistleblower) Policy*, whistleblower protections and processes

- 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
- notify the regulatory authority within 24 hours, via NQA ITS, if a child is involved in a serious incident, including any unsafe online interactions, exposure to inappropriate content or suspected online abuse.

Physical Environment and Supervision

- reflect on the Service's physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology
    - 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'
    - ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members when working with children
    - only permit children to use devices in open areas where educators can monitor children's use
    - 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
    - ensure all devices are password protected with access for staff only
- where Service-supplied digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure
- remind families that children enrolled at the Service are not permitted to bring electronic devices to the Service, unless an exception has been discussed with the approved provider or nominated supervisor where the device may be required to support a diagnosed medical condition or disability

Personal Device Restrictions

- ensure all staff, educators, volunteers and students adhere to National Law legislation and regulator directions regarding the supply, authorisation and use of electronic devices
- inform all staff, educators, visitors and volunteers that use of personal electronic devices to capture, store or transfer images or videos of children being educated and cared for by the Service is strictly prohibited
- ensure personal electronic devices are not in the possession of any relevant person involved in the operation of the Service while working directly with children
- relevant persons include approved providers, service leaders, educators, employees, volunteers, or visitors (e.g. ECIP professionals) while working directly with children
- restrictions do not apply to people who do not work directly with children and who are not providing education and care
- any 3rd party professional (NDIS funded support professionals, Inclusion Support Professionals) can only use a device that is issued by their business or institution and this must be a work-only device and not used for personal use
- legislative restrictions do not apply to families who are dropping off or collecting their child from the Service
- inform staff that they may be in the possession of their personal device during a break, provided no enrolled children are present or have access to the staff room

Exemptions for Use of Personal Devices

- the approved provider may grant written exemptions permitting a person to use or be in possession of an electronic device while working directly with children for prescribed circumstances
- a person with an exemption must not use the personal device to take images or video of children while working directly with children
- exemptions may apply when required for operational activities, for example during excursions or when providing transportation where the device is necessary for the purposes of safety or the provision of education and care to the children.

- Risk assessments should consider if a service-issued device will be sufficient to meet the safety requirements of all children without a reliance on personal devices.

Exemptions 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)

- exemptions for prescribed circumstances must be reviewed every 3 months
- written authorisations must be retained for a period of 3 years
- an additional prescribed circumstances may apply if a Service-supplied or issued device stops working and another device is temporarily required
- approved providers may revoke authorisations as required, ensuring that all revocations are properly documented
- written prescribed circumstance authorisations must include approved provider details, person's details (including name and role), name of person making the authorisation, description of personal device, reasons for the authorisation and duration of the authorisation.

Service-supplied Devices

- ensure staff and educators only use Service-supplied or issued devices for taking images or videos of children
- ensure all devices purchased for the Service are recorded via the *Electronic Service-Supplied Device Form*
- ensure the *Electronic Service-Supplied Device Form* includes the date of supply, type of device, make, model, serial number, name and signature of approved provider supplying the device and a declaration that the device is configured to operate in line within this policy
- create and maintain a register for all service-supplied electronic devices used at the Service including records of allocation, use and return
- the *Electronic Device Register* should include type of device, unique identifier (e.g. asset number), who device is allocated to, dates of allocation and return (revocation records)
- records relating to the supply or issue of electronic devices, should be stored securely a for a period of 3 years from the date the record was made
- electronic devices supplied or issued by and registered with the Service will be stored in a secure location
- document a record of revocation for any electronic devices no longer used in the Service
- ensure Service-supplied devices are configured, monitored and maintained to prevent unauthorised access or misuse

Images, Videos and Authorisation

- determine who is authorised to capture, use, store and destroy images and videos of children using Service-supplied devices
- inform parents/guardians during enrolment and orientation how the Service will capture, use, store and destroy images and videos
- request written authorisation from families to capture, use, store and destroy digital documentation including images and video of children at time of enrolment
- ensure images or videos of children are not taken, used or stored without prior parent/guardian authorisation
- develop, maintain and share a confidential record of all children who are NOT to be photographed or videoed
- obtain written authorisation from parents/guardians for children to use electronic devices

- obtain written authorisation to collect and share personal information, images or videos online (Service website or Storypark)
- seek written authorisation from parents/guardians when an outside photographer/agency is contracted to take photographs 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. [See *Media Authorisation Form*]
- ensure children without photography authorisation are provided with alternative activities during external photography sessions
- ensure ECIP visitors gain authorisation from both the approved provider and parent/guardian prior to taking images or video of children whilst at the Service
- ensure staff, educators, visitors and volunteers do not transfer images or videos from Service-supplied devices to personal devices. Unauthorised transferring of digital data may result in disciplinary action.

Data and Privacy

- ensure the *Privacy and Confidentiality Policy* is adhered to at all times
- ensure images and videos will be stored securely with password protection, with access limited to authorised persons only
- back-ups of all digital data, whether offline or online (such as a cloud-based service), will be performed each month
- digital data stored at the Service will be deleted and destroyed in accordance with the *Record Keeping and Retention Policy*
- ensure every child is protected from exploitation of photographic and video images
- ensure images or videos do not show children in distress, in positions that may be perceived as sexualised or in a state of undress
- 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, then destroyed
- processes must ensure families who speak languages other than English understand the authorisation requirements
- notify the Office of the Australian Information Commissioner (OAIC) in the event of a possible data breach by using the online Notifiable Data Breach Form. This could include:
  - 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)
  - a data base with personal information about children and/or families is hacked
  - personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)
  - any possible breach within the Service or if the device is left behind whilst on an excursion.

EDUCATOR RESPONSIBILITIES

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
- be aware of current child protection law, National Principles for Child Safe Organisations and Child Safe Standards and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- 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 our Service's operations, including when accessing digital technologies and online learning environments
- not use, or have access to, any personal electronic devices while working directly with children, unless an exemption has been authorised
- not access personal social media on any device while working directly with children

- keep passwords confidential and log out of computers and software programs
- 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 images and video 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
- ensure children's personal identifiable information is not shared online
- ensure screen time is NOT used as a reward or to manage challenging behaviour
- follow the Service's *Educational Program Policy* regarding recommended screen time limits and sedentary behaviour of children
- ensure any digital media, television programs or online content accessed at the Service will be age-appropriate, culturally respectful and consistent with the Service's *Educational Program*
- introduce concepts about online safety to children at age-appropriate levels
- consult with children about matters that impact them, including the use of online environments
- report any concerns related to child safety, including inappropriate use of digital technology to the approved provider or nominated supervisor.

Families will:
- adhere to this policy and associated procedure
- not use personal electronic devices to take photos, record audio or capture video of children being educated and cared for at the Service
- provide written authorisation indicating whether or not the Service may take, use, store or destroy images or videos of their child
- provide written notification if they wish to withdraw the authorisation at any time
- be requested to provide written authorisation/consent for individuals visiting the Service to take photographs of their child/ren (e.g., ECIP professionals, professional photography for marketing, school photos etc.)
- be aware that other children may feature in the same photos, videos and observations as their child, and not duplicate or upload these to the internet or social networking sites.

Visitors, Volunteers and Students will:
- adhere to this policy and associated procedure whilst visiting the Service
- not use personal electronic devices to take photos, record audio or capture video of children being educated and cared for at the Service
- report any concerns related to child safety, including inappropriate use of digital technology to the approved provider or nominated supervisor
- obtain written authorisation from parents/guardians and the approved provider before capturing images or video of a child (applies to NDIS funded support professionals, Inclusion Support professionals and other ECIP visitors) (See *ECIP Confidentiality Agreement*).

SOFTWARE PROGRAMS AND APPLICATIONS

Our Service uses a range of secure software programs and apps on service-supplied or issued devices to support the educational program and administration of the Service.
- All applications used by staff, educators, visitors and children must be carefully selected, regularly checked and kept up to date
- Access to software programs and applications must be password protected
- Each user must create their own user account and not share information
- Educational program software used by educators to share observations, photos, videos, daily reports, and learning portfolios with families will be hosted on a secure, closed and authorised platform
- Programs requiring additional background checks (such as Department Software) must only be accessed by authorised staff who have completed necessary screening processes

ARTIFICIAL INTELLIGENCE (AI) USE

Educators or staff using AI must be aware of limitations, privacy risks, and the potential for errors in the information it provides.

- AI may be used to support documentation tool; however, educators and staff must verify accuracy and not rely upon AI as an authoritative source
- Educators and staff must enter original work and verify that information obtained from AI is contextually relevant
- Educators and staff must not enter personal or identifying details of individual children (such as names and dates of birth) into AI tools.
- Data and privacy concerns must be addressed in accordance with this policy and the *Privacy and Confidentiality Policy.*

BREACH OF POLICY

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. Visitors or volunteers who fail to comply to this policy may face termination of their engagement. 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 Service.

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/

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Safe Use of Digital Technologies and Online Environments Policy* will be reviewed on an annual basis or earlier if there are changes to legislation, ACECQA guidance or any incident related to our policy. Feedback will be requested from children, families, staff, educators and management and notification of any change to policies will be made to families within 14 days.

SOURCES

Australian Children's Education & Care Quality Authority. (2023). Embedding the National Child Safe Principles
Australian Children's Education & Care Quality Authority. (2026). Guide to the National Quality Framework
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.(2026). Using digital devices in centre-based education and care services 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. (2026). 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

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/
Children (Education and Care Services) National Law (NSW)
Early Childhood Australia (2016). *Code of Ethics.*
Education and Care Services National Law Act 2010
Education and Care Services National Regulations 2011
Education and Care Services National Regulations (NSW) (2025)
NSW Government. (2026). Ministerial Direction. Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026
Office of the Australian Information Commissioner (OAIC)
Privacy Act 1988.