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 [Vic] 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 systems	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	
S. 162A	Child protection training
S. 162B	Child safety training
S. 165	Offence to inadequately supervise children
S.166	Offence to use inappropriate discipline
S. 166A	
S. 167	Offence relating to protection of children from harm and hazards
PART 6A	Devices in education and care services
12	Meaning of serious incident
73	Educational Program
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
128B	Child protection training
128D	Foundation child safety training
128E	Advanced child safety training
149	Volunteers
168	Education and care service 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
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

RELATED LEGISLATION

Child Care Subsidy Secretary's Rules 2017	*Privacy Act 1988* (Cth)
Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook	Surveillance Devices Act 2004 (Cth)

RELATED POLICIES

Behaviour Guidance: Bullying Policy Child Safe Environment Policy Child Safety and Wellbeing Policy (VIC) Child Protection Policy Code of Conduct Policy Dealing with Complaints Policy	Fraud Prevention Policy Incident, Injury, Trauma, and Illness Policy Interactions with Children, Families and Staff Policy Physical Activity Policy Privacy and Confidentiality Policy

Early Childhood (ECIP) Intervention Practitioner Management Policy Educational Program Policy Enrolment Policy Family Communication Policy Governance Policy	Protected Disclosures (Whistleblower) Policy Record Keeping and Retention Policy Staffing Arrangements Policy Student, Volunteer and Visitors Policy Supervision Policy Social Media 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 safety culture that supports our Service philosophy and complies with privacy and legislative requirements to ensure the safety of enrolled children, educators and families.

This policy provides the framework and guidance for the safe use of digital technologies and online environments at the Service, including:

- the capture, use, storage and destruction of images and videos of children being educated and cared for by the Service
- obtaining written authorisation from parents/guardians to take, use and store images and videos of children
- the use of any digital device issued by the Service
- the use of digital devices by children being educated and cared for at the Service, including augmentative and alternative communication (AAC) devices
- 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 For additional definitions and key terms used within this policy, refer to *Key Terms – Policies and Procedures.*	
Augmentative and alternative communication (AAC) devices	Devices that support a child to use language and communicate other than through spoken speech. AAC devices may include tablets, computers, speech-generating devices, and other electronic communication aids.

Artificial intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation.
Capturing	Includes filming, recording or taking a photo/image of a child.
Cyberbullying	The use of digital technologies or online platforms to harass, threaten, humiliate or harm a child or young person
Cyber safety	Safe, secure and responsible use of the internet and electronic equipment/devices, including mobile phones.
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 abused, or by which an adult conveys or attempts to convey that they were sexually abused as a child. This may take many forms, and might be verbal or non-verbal. Non-verbal disclosures using painting or drawing, gesticulating, or through behavioural changes, are more common among young children and children with cognitive or communication impairments.
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, including digital devices, systems, networks and software used to create, access, store, communicate or manage information
Illegal content	Content that includes images and videos of child sexual abuse, content that includes or advocates 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	Photographs, images or video recordings of children taken while they are being educated and cared for by the Service, whether captured on a service-supplied or personal.
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
Optical surveillance device	A device used for visual monitoring or observation, including closed-circuit television (CCTV) systems.
Personal electronic devices	Devices owned by a person (NOT owned/supplied by an approved provider for education and care purposes) and are capable of capturing, storing or transmitting an image or video. Examples include mobile phones, cameras,

	tablets, smartwatches, smartglasses, storage media such as SD/memory cards, USB drives, hard drives and other new emerging devices.
Service-supplied devices	A device owned or supplied by an approved provider to be exclusively used 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. A service-supplied device must not be used for personal purposes.
Sexting	Sending a sexual message or text, with or without a photo or video, using a phone service or any platform that allows people to connect via online messaging or chat
Smart toys	Smart toys are toys that connect to the internet or other technology to provide interactive or digital functions and may collect, store or transmit information.
Storing	Storing means keeping the photo/image or video saved on a device, including a storage device.
Software platforms	Digital programs, applications or systems used by the Service for education and care, administration, communication, recordkeeping or other Service functions. This includes Child Care Subsidy (CCS) software, programming platforms and other online applications or systems used by the Service.
Transmitting	Includes sharing a photo by text message, email, USB/hard drive, uploading to any 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: Terminology adapted from ACECQA's *Safe Use of Digital Technologies and Online Environments Policy and Procedure Guidelines*, *Guide to the NQF* and other relevant resources.

IMPLEMENTATION

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

Our Service uses digital technologies, including electronic devices, software and online environments, 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. These 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, where relevant, are met
- ensure educators, staff, students, visitors and volunteers have access to, understand and adhere to this policy and other related policies and procedures
- 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 relevant persons complete the required child safety and child protection training within the prescribed timeframes (see *Child Protection Policy*)
- ensure child safe practices are embedded into organisational practice as per National Principles for Child Safe Organisations [Vic]
- 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 and online environments.

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 related procedures as part of their induction and are advised on how and where these can be accessed
- provide professional learning to educators and staff regarding the safe use of digital technologies and online environments.

Child Safe Culture

- ensure all staff, educators, students and volunteers are aware of their child protection obligations and, where applicable, 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, and relevant authorities (see *Child Protection Policy*)

- maintain required educator to child ratios and active supervision at all times, including when children are using digital technologies.
- ensure all students, visitors and volunteers comply with the Service's requirements for the safe use of digital technologies and online environments, are supervised at all times and are never left alone with a child.
- conduct risk assessments to identify and manage risks associated with the use of digital technologies and online environments.
- review risk assessments annually or as soon as practicable after becoming aware of circumstances that could affect child safety
- ensure a review of practices is conducted following an incident involving digital technologies and online environments, including consideration of areas for improvement
- ensure reasonable precautions are taken to prevent personal device use in breach of National Law, National Regulations and regulator directions (Vic)
- implement reasonable measures to protect digital technologies, devices, systems and information from unauthorised access, inappropriate use and security threats, such as installing and maintaining anti-virus and internet security systems, including firewalls to block access to unsuitable websites, newsgroups and chat rooms, and requiring strong passwords and multi-factor authentication where available, and locking devices when unattended
- support educators to:
    - encourage children to seek support if they encounter anything that makes them feel uncomfortable, scared or upset
    - listen sensitively and respond appropriately to any concerns or disclosures children may make relating to unsafe online interactions or exposure to inappropriate content, adhering to the *Child Protection Policy, Behaviour Guidance: Bullying Policy* and relevant reporting procedures
    - respond to and report any breaches and incidents of inappropriate use of digital technologies and online environments to management
- ensure all concerns, incidents and disclosures 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 and other reportable matters to the relevant authorities, including the e-Safety Commissioner and Police, in accordance with applicable legislation and the Service's *Child Protection Policy* and related procedures

- notify the regulatory authority if a child is involved in a serious incident, including serious injury or trauma or incidents involving unsafe online interactions, exposure to inappropriate content or suspected online abuse through the National Quality Agenda IT System (NQA ITS), and to the child's parents/guardians within the prescribed timeframes.

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 digital technologies
  - perform regular checks and audits of room layouts and technology use to identify potential risks to children's safety, such as potential supervision blind spots, and make necessary changes
  - ensure the 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 and support 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.
- ensure that 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 procedures
- 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 child's diagnosed medical condition or disability, such as devices used to support communication, or other accessibility requirements.

Personal Device Restrictions

- ensure all staff, educators, volunteers and students adhere to National Law, National Regulations and regulator directions, if applicable, regarding the supply, authorisation and use of electronic devices
- inform all staff, educators, visitors and volunteers of the Service's requirements regarding personal electronic devices, including that use of personal electronic devices to capture, store or transmit 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 while working directly with children at the Service

- ensure third-party professionals (e.g., NDIS-funded support professionals or inclusion support professionals) comply with the Service's requirements and only use a device that their business or institution issues, and this must be a work-only device and not used for personal use
- inform staff that they may be in possession of their personal device during a break, provided no enrolled children are present or have access to the staff room
- let families know that while legislative restrictions on personal device possession do not apply to them when dropping off or collecting their child, they must be cautious when using personal devices around children and comply with the Service's requirements regarding photography, recording and privacy.

Authorised Exceptions for Personal Device Use

- ensure written authorisations are provided by the approved provider (where applicable) for prescribed circumstances permitting a person to use or be in possession of a personal electronic device while working directly with children, including:
    - providing support or assistance with the person's disability or health needs (e.g., heart or blood sugar monitoring)
    - communication with a family member of the person. This should only be used in limited circumstances, e.g., urgent family matters.
    - safety or the provision of education and care to the children if a service-supplied device ceases working
    - use in an emergency, e.g., during incidents such as a lost child, injury, lockdown, or evacuation and local emergency events to receive alerts (e.g., government bushfire or evacuation notifications)
    - for work health and safety reasons, e.g., when required for operational activities, for example during excursions or when providing transportation where the device is necessary for safety or the provision of education and care to the children.
- ensure risk assessments consider if a service-supplied device will be sufficient to meet the safety requirements of all children without a reliance on personal devices during excursions and transportation
- ensure written authorisations are given in advance for the above purposes, except in circumstances where it is not practical to give prior authorisation, such as in emergencies
- ensure written authorisations given by the approved provider include the approved provider's

details, the details of the person authorised to possess or control the personal device, including their name and role, the name of the person making the authorisation, a description of the personal device, the reasons for the authorisation and duration of the authorisation

- ensure a person with an authorisation does not use the personal device to capture, store or transmit images or video of children while working directly with children
- retain written authorisations for a period of 3 years
- revoke authorisations within 48 hours of becoming aware that there is no valid reason to continue the authorisation and ensure any revocation of an authorisation is properly documented.

Service-supplied Devices

- ensure staff and educators only use service-supplied devices for capturing images or videos of children
- ensure all electronic devices supplied by the Service are recorded in writing, e.g., via the *Electronic Service-Supplied Device Record and Register*, including the date of supply, type of device, make, model, serial number, Service details, including the name and signature of the approved provider supplying the device, and a declaration that the device is configured to operate in line with this policy and other related child safe policies; and, where applicable, details of the revocation of the device, including the reason, date, and approved provider's name and signature.
- create and maintain a register for all service-supplied electronic devices used at the Service including records of allocation, use and return [see *Electronic Service-Supplied Device Record and Register]*
- ensure the register includes the type of device, unique identifier (e.g. asset number), person the device is allocated to and dates of allocation and return (revocation records)
- securely store records relating to the supply of electronic devices for a period of 3 years from the date the record was made
- securely store service-supplied electronic devices when not in use e.g., in a locked cabinet at the end of the day
- document the revocation of any electronic devices no longer used by the Service [best practice]
- ensure service-supplied electronic devices are configured, monitored and maintained to prevent unauthorised access or misuse
- ensure a service-supplied device is not shared across multiple services. Some exemptions apply. [check with your regulatory authority]

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 about how the Service will capture, use, store and destroy images and videos of children
- obtain written authorisation from parents/guardians, where required, for:
    - capturing, using, storing and destroying images and videos of children during the provision of education and care
    - collecting and sharing personal information, images or videos online, including through the Service website, Facebook, Instagram or [enter name of parent communication app]
    - children to participate in external photography, including individual or group photographs and photography for marketing purposes (see *Media Authorisation Form*)
    - children to use electronic devices (see *Cyber Safety Authorisation*)
- ensure images or videos of children are not captured, used, stored or shared without the required parent/guardian authorisation
- develop, maintain and share a confidential record of all children who are not authorised to be photographed or videoed, and ensure children without photography authorisation are provided with alternative activities during external photography sessions
- ensure ECIP professionals obtain authorisation from both the approved provider and parent/guardian prior to taking images or video of children while at the Service
- ensure staff, educators, visitors and volunteers do not transfer images or videos from service-supplied devices to personal devices. Unauthorised transfer 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 are stored securely using password protection, with access limited to authorised persons only
- perform monthly back-ups of all digital data, whether stored offline or online (such as a cloud-based service)
- ensure digital data stored at the Service is 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 and videos do not show children in distress, in positions that may be perceived as sexualised or in a state of undress
- retain images and videos that form part of a record, such as records relating to a child or staff member, for the applicable record retention period; after the required retention period, securely delete or destroy these images and videos from all relevant storage locations and formats, including electronic and physical copies
- securely delete or destroy images and videos that do not form part of a record, or that are no longer required for the purpose for which they were taken
- notify the 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 database with personal information about children and/or families is hacked or accessed without authorisation
    - personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)
    - a device containing personal information is left behind during an excursion or other Service activity.

EDUCATOR RESPONSIBILITIES

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedures
- understand and comply with their child protection obligations and, where applicable, mandatory reporting obligations, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- complete the required child safety and child protection training within the prescribed timeframes (see *Child Protection Policy*)
- participate in practical training related to digital safety, privacy protection and responsible use of technology
- 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 authorised by the approved provider or in other prescribed circumstances
- not access personal social media on any device while working directly with children

- keep passwords confidential and log out of computers and software programs when not in use
- comply with the Service's authorisation requirements before taking images or videos of
- ask permission before taking images or videos of children on any device and explain to children, in an age-appropriate way, how images and videos of them will be used and where they may be published
- ensure images and videos do 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 without appropriate authorisation
- ensure images, videos and personal information are not transferred from service-supplied devices to personal devices or accounts.
- ensure screen time is not used as a reward or to manage challenging behaviour
- follow the Service's *Physical Activity Policy* regarding recommended screen time limits and sedentary behaviour of children
- ensure any digital media, television programs or online content accessed at the Service are age-appropriate, culturally respectful and consistent with the Service's *Educational Program and Physical Activity Policies*
- introduce concepts about online safety to children at age-appropriate levels
- consult with children about matters that affect 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, and relevant authorities (see *Child Protection Policy*).

VISITORS, VOLUNTEERS AND STUDENTS WILL:

- adhere to this policy and associated procedures while visiting or working at the Service
- volunteers and students will complete the required child safety and child protection training within the prescribed timeframes (see *Child Protection Policy*) and comply with their child protection obligations and, where applicable, mandatory reporting obligations and duty of care to take reasonable steps to prevent harm to children
- obtain written authorisation from parents/guardians and the approved provider before capturing images or videos of a child (applies to NDIS-funded support professionals, inclusion support professionals and ECIP professionals) (See *ECIP Confidentiality Agreement*)
- not use personal electronic devices to take images, record audio or capture video of children being educated and cared for at the Service
- maintain confidentiality and not disclose or share personal information, images or videos of children outside the Service unless authorised by the Service or required by law

- 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 procedures
- not use personal electronic devices to take images, record audio or capture video of children being educated and cared for at the Service.
- provide written authorisation, where required, 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 or change their authorisation at any time
- provide written authorisation for individuals visiting the Service to capture images or videos of their child/ren (e.g., ECIP professionals, professional photography for marketing, school photos etc.)
- take care when uploading or sharing images, videos or other information through Service-approved communication platforms, considering the privacy, dignity and safety of all children, including their own child
- be mindful when using personal electronic devices at the Service and take reasonable steps to protect children's privacy and safety
- be aware that other children may feature in the same images, videos and observations as their child, and not copy, share or upload these, or any information identifying other children, to the internet or social networking sites.

SOFTWARE PROGRAMS AND APPLICATIONS

Our Service uses a range of secure software programs and applications on service-supplied devices to support the educational program and administration of the Service.

- Only service-approved software programs and applications are used on service-supplied devices
- All applications used by staff, educators, visitors and children are carefully selected, regularly reviewed for suitability and security, and kept up to date
- Access to software programs and applications is password protected
- Each user has an individual user account and does not share login details or account access with others
- Educational program software used by educators to share observations, images, videos, daily reports, and learning portfolios with families is hosted on a secure, service-approved platform

- Programs requiring additional background checks, such as Child Care Subsidy (CCS) software, are only accessed by authorised staff who have completed the necessary screening processes in accordance with Family Assistance Law
- Software programs and applications that are no longer required, supported or considered suitable are removed from service-supplied devices.

ARTIFICIAL INTELLIGENCE (AI) USE

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

- AI may be used to support documentation; however, educators and staff must verify the accuracy of AI-generated information and not rely upon AI as an authoritative source
- Educators and staff must use their professional judgement when using AI and verify that information obtained from AI is accurate, appropriate and contextually relevant
- Educators and staff must only use AI tools approved by the Service and must not enter personal or identifying information about children, families or staff, such as their names and dates of birth, images or videos 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 employment obligations and may face disciplinary action. Serious breaches may result in notification to the regulatory authority or other relevant authorities where required.

Visitors, volunteers and students who fail to comply with this policy may face termination of their engagement.

Family members who do not comply with this policy may have their access to Service facilities or communication platforms restricted, where reasonably necessary to protect children's safety, privacy and wellbeing.

RESOURCES

eSafety Commissioner. Early Years program for educators

eSafety Commissioner. eSafety checklist for early learning services

eSafety Commissioner. Our Family Tech Agreement

eSmart Allanah & Madeline Foundation. eSmart Resources

Kiddle. Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Safe Use of Digital Technologies and Online Environments Policy* will be evaluated and 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. All families will be notified 14 days before any policy change that may have a significant impact on the provision of education and care to any child enrolled at the Service or the family's ability to utilise the Service, or earlier in line with the *Governance Policy*.

RELATED RESOURCES

CCS Compliance Checklist CCTV Monitoring Letter to Families Cyber Safety Agreement Cyber Safety Authorisation Data Breach Response Plan Record Data Security Checklist Digital Technologies and Online Environments - Risk Assessment ECIP Confidentiality Agreement	Electronic Device Authorisation Record and Register Electronic Service-Supplied Device Record and Register Media Authorisation Child Media Authorisation Staff Privacy Audit Privacy and Confidentiality Procedure Safe Use of Digital Technologies and Online Environments Procedure

SOURCES

Australian Children's Education & Care Quality Authority. (2026). *Guide to the National Quality Framework*
Australian Children's Education & Care Quality Authority. (2025). *NQF Online Safety Guide*
Australian Children's Education & Care Quality Authority. (2026). *Using digital devices in centre-based education and care services*
Australian Government. Department of Education. (2026). *Child Care Provider Handbook*
Australian Government. Department of Health, Disability and Ageing. (2026). *24-hour movement guidelines for all Australians*
Australian Government. eSafety Commissioner. (n.d.) *Report online harm*
Australian Government. Office of the Australian Information Commissioner. (2026). *Australian Privacy Principles guidelines*
Australian Human Rights Commission. *(n.d.) Child Safe Organisations.*
Education and Care Services National Law Act 2010
Education and Care Services National Regulations 2011

NSW Government. Early Learning Commission. (2026). *Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026*
NSW Government. Education (2026). *Restriction on personal devices*
Privacy Act 1988.

REVIEW

POLICY REVIEWED BY	[NAME] Amy Flockhart	[POSITION] office admin	[DATE] 08/10/2026
POLICY REVIEWED	OCTOBER 2026	NEXT REVIEW DATE	OCTOBER 2027
VERSION NUMBER	V5.10.26		
MODIFICATIONS	• annual policy review • adjusted definitions and added definitions for AAC devices, storing and software platforms • authorised exceptions for personal device use section adjusted • updated information about service-supplied devices, personal devices, written authorisations and registers • strengthened active supervision of children using digital technologies and online environments, child protection obligations and reporting of concerns • updated responsibilities sections for clearer expectations • updated information about privacy, cybersecurity and the use of AI • checked and updated resources and references		
PREVIOUS MODIFICATIONS			
MARCH 2026	• major rewrite of policy draft to align with recent amendments to National Law, including the introduction of Part 6A and other child safety provisions such as paramount consideration • additional directions and definitions of personal devices from ACECQA (2026) have been included. • subheadings added to assist with grouping responsibilities for the approved provider and management • Services must contextualise to their own requirements		