P-2.28 Safe Use of Digital Technologies and Online Environments

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

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 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.
	Child Safety and Protection (effective Jan 2026)	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 2: 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. 162A	Child protection training
S. 165	Offence to inadequately supervise children
S. 166A	Offence to subject child to inappropriate conduct [NSW]
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

RELATED POLICIES

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

P-2.28 Safe Use of Digital Technologies and Online Environments

CCS Data Security Policy CCS Personnel Policy CCS Account Policy Providing a Child Safe Environment Policy Child Protection Policy Code of Conduct Policy Dealing with Complaints Policy Educational Programs Policy Enrolment Policy Family Communication Policy Governance and Leadership Policy	Fraud Prevention Policy Incident, Injury, Trauma, and Illness Policy Interactions with Children Families and Staff Policy Photograph and Social Media Policy Technology and Media Policy Privacy and Confidentiality Policy Programming Policy Record Keeping and Retention Policy Staffing Arrangements Policy The Participation of Volunteers, Students and Visitors Policy Supervision Policy

DEFINITIONS

Artificial intelligence (AI)	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given sent of human defined objectives or parameters without explicit programming.
Cyberbullying	When someone uses the internet to be mean to a child or young person so they feel bad or upset
Cyber safety	Safe and responsible use of the internet and equipment/devices, including mobile phones and devices.
Disclosure	Process by which a child conveys or attempts to convey that they are being or have been sexually abuses, or by which an adult conveys or attempts to convey that they were sexually abused as a child
Generative artificial intelligence (AI)	A branch of AI that develops generative models with the capability of learning to generate novel content such as images, text and other media with similar properties as their training data
Harmful content	Harmful content includes sexually explicit material; false or misleading information; violence; extremism or terrorism; hateful or offensive material
ICT	Information and Communication Technologies
Illegal content	Includes: images and videos of child sexual abuse Content that advocates terrorist acts Content that promotes, incites or instructs in crim or violence Footage of real violence, cruelty and criminal activity
Optical Surveillance Device	Has the same meaning as in section 6(1) of the Surveillance Devices Act 2004 of the Commonwealth
Online hate	Any hateful posts about a person or group based on their race, religion, ethnicity, sexual orientation, disability or gender
Smart toys	Smart toys generally require an internet connection to operate as the computing task is on a central server
Sexting	Sending a sexual message or text, with or without a photo or video. It can be done using a phone service or any platform that allows people to connect via an online message or chat function
Unwanted contact	Any type of online communication that makes you feel uncomfortable, unsafe or harassed.

PURPOSE

Children's safety and wellbeing is paramount and our OSHC Service has the responsibility to provide and maintain a safe and secure working and learning environment for staff, children, visitors and contractors, including online environments. We aim to create and maintain a positive digital safe culture that works in conjunction with our OSHC 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.

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

P-2.28 Safe Use of Digital Technologies and Online Environments

SCOPE
This policy applies to all DEBASCA stakeholders.

RESPONSIBILITIES
Responsibility for implementation of this policy lies with the Director or other authorised representative approved by the Director and the Management Committee.

TRAINING REQUIREMENTS
Personnel having responsibilities under this procedure will be appropriately trained.

IMPLEMENTATION

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

PROCEDURE

1. **Digital Technology and Electronic Devices used at the Service**
   1.1. Our Service adopts and aligns with the National Model Code and Guidelines for taking images or videos of children. Our Service ensures compliance with the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025.
   1.2. The approved provider will inform staff, educators, visitors, volunteers and family members that the use of personal electronic devices used to take, store or transfer images or videos of children who are being educated and cared for at the Service is strictly prohibited. This includes items such as tablets, mobile phones, computers/laptops, digital cameras, smart watches, META sunglasses and personal storage and file transfer media (such as SD/memory cards, USB drives, hard drives and cloud storage). These devices should not be in the possession of staff, educators or visitors while working directly with children, including during excursions or when children are being transported.
   1.3. Staff and educators are advised that electronic devices supplied or issued by and registered with the Service must not be removed from the premises as they may contain personal details of staff or children, including photos or videos. Except where required and approved for operational activities, for example excursions or transportation.

2. **Exemptions**
   2.1. The approved provider will inform staff, educators and visitors of exemptions or prescribed circumstances that may warrant a person to use or be in possession of a personal electronic device that can be used to take images or videos. Staff, educators or visitors with an exemption must not use the personal device to take images or videos while working directly with children. Exemptions need to be provided for in writing by the approved provider and may include:
      2.1.1. Emergency communication during incidents such as a lost child, injury, lockdown, or evacuation
      2.1.2. Personal health needs requiring device use (e.g. heart or blood sugar monitoring)
      2.1.3. Disability related communication needs
      2.1.4. Urgent family matters (e.g. critically ill or dying family member)
      2.1.5. Local emergency event to receive alerts (e.g. government bushfire or evacuation notifications)

3. **Additional practices for NSW Services only:**
   3.1. 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 Service details, person's details, reasons for the authorisation and duration of the authorisation.

4. **Service-Supplied or Issued Electronic Devices**
   4.1. Service-supplied or issued devices must be configured to comply with Service policies and procedures as outlined within this policy.
   4.2. Our Service will maintain records of electronic Service-supplied devices including the date of supply, type of device,

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

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.

4.3. If the device is no longer used within the Service, a record of revocation will be documented. This is mandatory for NSW services, recommended best practice for other states/territories.

4.4. Our Service will develop and maintain a register of all electronic devices purchased for and used within the Service. Each device purchased for and used at the centre will be clearly marked with an identification code and marked to state it is property of the Service. This register will include details such as the identification code, device type, date of purchase, intended use, assigned user (if applicable), security settings, and any features related to connectivity, data storage, or recording capabilities.

4.5. Devices recorded in the register may include, but are not limited to, computers, tablets, mobile phones, cameras, CCTV systems, audio recorders, smart toys, baby monitors and any other internet-connected or data-enabled devices used within the Service.

4.6. Electronic devices issued by and registered with the service will be stored in a locked cabinet at the end of the day. Records relating to the supply or issue of electronic devices, including registers of use Service-supplied or issued device is to be stored securely for a period of 3 years from the date the record was made.

5. Children Bringing Personal Devices to the Service

5.1. Children enrolled at our OSHC Service are not permitted to bring personal electronic devices, including but not limited to laptops, mobile phones, smart watches, tablets and/or smart glasses to the Service; unless an exception has been discussed with the nominated supervisor where the device may be required to support a diagnosed medical condition or disability, or for other authorised purposes.

5.2. If a child brings an electronic device to the Service, it will be stored in a locked cupboard/office to be collected at pick up time.

5.3. Parents wishing to contact their children should do so via the service landline or email, and a message will be passed on to their child.

5.4. Children are strictly prohibited from wearing or bringing in a pair of smart glasses (eg: Meta glasses) to the service.

5.5. Under no circumstance should a child record, or store images of another child and/or educator/parent whilst at the service

5.6. Any child found in breach of this policy by misusing a device may face disciplinary action.

6. Images and Videos

6.1. The approved provider is responsible for determining who is authorised to take, use, store and destroy images and videos of children using Service-supplied or issued digital devices. Images and videos will be stored securely with password protection, with access limited to authorised personnel only. Images and videos of children must only be taken and used in accordance with the Service's policies, and careful consideration given to the purpose of the image or video. Educators will engage in discussions that consider the intent, appropriateness, context and consent involved in capturing and using the images and videos, ensuring the process aligns with children's learning, wellbeing and right to privacy.

6.2. Our Service will regularly review how digital data, including images and videos of children, is stored. Back-ups of all digital data, whether offline or online (such as a cloud-based service), will be performed regularly. Digital data stored at the Service will be destroyed in accordance with the *Record Keeping and Retention Policy* and procedure. The approved provider will ensure staff, educators, visitors and volunteers do not transfer images or videos from Service issued devices to personal devices, unauthorised transferring of digital data may result in disciplinary action.

7. Physical Environment and Active Supervision

7.1. **The approved provider, nominated supervisor, management and educators will:**

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

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

7.1.3. reflect on the physical environments used by the Service, the layout and design to ensure it supports child safe practices when children are engaged in using technology

7.1.4. perform regular audits to identify risks to children's safety and changes in room set-ups that can indicate

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

areas of higher-risk and become supervision 'blind spots'

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

7.1.6. only permit children to use devices in open areas where educators can monitor children's use

7.1.7. 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

7.1.8. ensure all visitors and volunteers are supervised at all times

7.1.9. ensure all devices are password protected with access for staff only

7.1.10. where digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure.

8. Software Programs and Apps

8.1. 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 apps used by staff, educators, visitors and children are carefully selected, regularly checked and kept up to date with the latest available system updates. Access to software programs and apps are password protected to ensure the privacy of children, families and staff. Each user is required to create their own user account and ensure log in, and password information is not shared.

8.2. The approved provider will ensure programs which require additional background checks, such as CCS Software, are only accessed by authorised staff who have completed necessary screening processes in accordance with Family Assistance Law. Our educational program software is used by educators to share observations, photos, videos, daily reports, and learning portfolios with families in a secure, closed platform. In addition, our Service may use accounting and payroll software, HR systems, and compliance tools. These platforms assist in managing the Service's financial, staffing, and operational requirements. These too will be password protected.

9. Artificial Intelligence (AI) Interactions and Guidelines

9.1. Educators or staff using AI are to be aware of limitations, privacy risks, and the potential for errors in the information it provides. AI can support and assist staff as a documentation tool; however, it is their responsibility to ensure the information's accuracy and not rely upon it as an authoritative source. Staff and educators should ensure they enter original work into the AI program and are required to monitor, verify, and check information obtained from AI to ensure specific details are contextually relevant. Data and privacy concerns must be addressed, and staff should not enter details which may identify individual children, such as names and date of birth.

10. Confidential and Privacy Guidelines

10.1. Our *Privacy and Confidentiality Policy* applies to all use of digital technology and online environments. All staff, educators, and visitors must ensure that any information, images, or digital content related to children, families, and the Service is collected, stored, used, and shared in accordance with privacy legislation and Service procedures, to maintain confidentiality and protect the safety and wellbeing of children. The nominated supervisor will advise the approved provider as soon as possible regarding any potential threat to security information and access to data sensitive information. Our Service will follow practices outlined within *the Safe Use of Digital Technologies* and *Online Environments Procedure* to protect personal and sensitive digital data.

10.2. The approved provider will 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:

10.2.1. 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)

10.2.2. a data base with personal information about children and/or families is hacked

10.2.3. personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)

10.2.4. this applies to any possible breach within the Service or if the device is left behind whilst on an excursion

10.2.5. ensure educators are aware of their mandatory reporting requirements and report any concerns

10.2.6. related to child safety including inappropriate use of digital technology to the approved provider or nominated supervisor

11. Identification and Reporting of Online Abuse and Safety Concerns

11.1. Our Service will implement measures to keep children safe whilst using digital technology and accessing online

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

environments.

11.2. **The approved provider, nominated supervisor and management will:**

11.2.1. ensure all staff, educators, students and volunteers are aware of their mandatory reporting obligations and promptly report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor [See *Child Protection Policy*]

11.2.2. 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*, *Bullying Policy* and reporting procedures
- respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management

11.2.3. ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required

11.2.4. ensure all educators, staff, students and families are advised of the *Protected Disclosure (Whistleblower) Policy*, whistleblower protections and processes

11.2.5. report any suspected cases of online abuse to the relevant authorities, including the eSafety Commissioner and Police, in accordance with legal requirements and child protection procedures

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

12. THE APPROVED PROVIDER/NOMINATED SUPERVISOR/RESPONSIBLE PERSON WILL ENSURE:

12.1. that obligations under the *Education and Care Services National Law and National Regulations* are met

12.2. educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure

12.3. new employees, students and volunteers are provided with a copy of the *Safe Use of Digital Technologies* and *Cyber Safety Policy* and procedure as part of their induction and are advised on how and where the policy can be accessed

12.4. families are aware of this *Safe Use of Digital Technologies* and *Cyber Safety Policy* and procedure and are advised on how and where the policy can be accessed

12.5. all staff, educators, volunteers and students are aware of current child protection law, NSW Child Safe Standards and their duty of care to ensure that reasonable steps are taken to prevent harm to children

12.6. families are aware of this *Safe Use of Digital Technologies and Online Environments Policy* and procedure and are advised on how and where the policy can be accessed

12.7. 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

12.8. they promote and support a child safe environment, ensuring adherence to the *Child Safe Environment* and *Child Protection Policies*

12.9. the NSW Child Safe Standards are embedded into the organisational structure and operations

12.10. professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments

12.11. a *Supply. Authorisation and Use of Electronic Device Register* is developed and monitored for all electronic devices purchased and used at the Service.

12.12. all electronic devices purchased and supplied for the Service are recorded via this *Register* and a record of revocation is documented for any electronic devices no longer used at the Service

12.13. appropriate ratios and adequate supervision are maintained for children at all times including when using digital technology and accessing online environments

12.14. students, volunteers and/or visitors are never left alone with a child whilst at the Service under any circumstances

12.15. all staff, educators, volunteers and students are aware of the National Model Code and Guidelines and adhere to these recommendations for taking images or video of children including:

12.15.1. personal electronic devices or personal storage devices, that can take images or videos, are not used by educators, staff, visitors or volunteers when working directly with children

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

12.15.2. staff and educators only use electronic devices supplied or issued by the Service for taking images or videos of children enrolled at the Service

12.15.3. Service issued devices are securely configured, monitored and maintained to prevent unauthorised access

12.15.4. exemptions or prescribed circumstances are authorised, in writing, for staff to possess or control a personal device while working directly with children

12.15.5. visitors who are supporting children at the OSHC Service (NDIS funded support professionals, Inclusion Support Professionals) obtain written authorisation from parents/guardians to capture images or video of a child for observation/documentation purposes only.

12.16. children, educators and parents are aware of our 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*)

12.17. the Service's *Privacy and Confidentiality Policy* is adhered to at all times by staff, educators, families, visitors, volunteers and students

12.18. parents/guardians are informed of how the Service will take, use, store and destroy images and videos of children enrolled at the Service during enrolment and orientation

12.19. written authorisation is requested from families to take, use, store and destroy digital documentation including images and videos of children

12.20. images or videos of children are not taken, used or stored without prior parent/guardian authorisation

12.21. a record of all children who are NOT to be photographed or captured on video is to be developed, maintained and shared with educators and staff. This record will remain private and confidential.

12.22. written authorisation is obtained from parents/guardians for children to use electronic devices

12.23. written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (Website, or Audiri, OWNA)

12.24. that the Service seeks written authorisation from parents/guardians for their child to be photographed 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*]

12.25. that the children of parents/guardians who do not wish their child to be photographed or videoed are provided with other activities when an external photographer/agency is engaged

12.26. allied health/early childhood professionals visiting the Service must obtain authorisation from the approved provider and parent/guardian prior to taking images or videos of children whilst at the Service. Images and videos must NOT be taken on personal devices.

12.27. families are informed to withdraw authorisation, a written request is required

12.28. images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian

12.29. they review how images and videos are stored on a regular basis and ensure new educators and staff have access to relevant folders and files, if required, in accordance with their role

12.30. digital data is stored securely, whether offline or online, using a cloud-based service, and that data is archived regularly

12.31. images and videos are deleted or destroyed and removed from storage devices in accordance with the *Record Keeping and Retention Policy,* images and videos used for documenting children's learning and development must be held for 3 years after the child's last day of attendance

12.32. every child in our care is protected from any exploitation of photographic and video images of themselves whilst they attend the Service

12.33. images or videos of children must be appropriate in nature and must not show children in distress, in a position that may be perceived as sexualised or in a state of undress, including where genitalia may be exposed

12.34. external agencies or specialists are consulted if concerns are identified relating to online abuse, cyberbullying or digital safety risks

12.35. policies and procedures reflect a commitment to equity and diversity, protect children's privacy, and empower children to be independent

12.36. collaboration with relevant professionals, as required, to support equitable access to digital technologies for all children

12.37. they remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the Office of the Australian Information Commissioner (OAIC)

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

12.38.   a risk assessment is conducted regarding the use of digital technologies by staff and children at the Service, including accessing online environments

12.39.   risk assessments for digital technology and online environments are reviewed annually or as soon as possible after becoming aware of any circumstances that may affect the safety, health or wellbeing of children

12.40.   policies and procedures are reviewed following an identification of risks following the review of risk assessments relating to the use of digital technologies and online environments

12.41.   staff, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies and online environments

12.42.   a review of practices is conducted following an incident involving digital technologies or online environments, including an assessment of areas for improvement

12.43.   to install and maintain anti-virus and internet security systems including firewalls (where possible) to block access to unsuitable web sites, newsgroups and chat rooms

12.44.   educators are informed of, and adhere to recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines:

12.44.1. children 5-12 years of age should limit screen time for entertainment to no more than 2 hours a day

12.45.   they share information to families about recommended screen time limits based on *Australia's Physical Activity* and *Sedentary Behaviour Guidelines*

12.46.   the use of TV/iPad and watching DVD's is kept to a minimum, with programs chosen that are engaging and age appropriate to children. When used, the following conditions apply:

12.46.1. only 'G' rated television programs and movies will be viewed at the Service

12.46.2. programs depicting violence and/or inappropriate content (including graphic news reports) will not be shown

12.46.3. TV programs or videos will only be shown that have positive messages about relationships, family and life

12.46.4. all content will be socially and culturally considerate and appropriate

12.47.   they share information to families about recommended screen time limits based on *Australia's Physical Activity and Sedentary Behaviour Guidelines*

12.48.   all documentation and records relating to safe use of digital technologies are kept safe and secure for a period of 3 years following the child's last day of attendance

12.49.   a review of practices is conducted following an incident involving digital technologies and online environments, including an assessment of areas for improvement.

13. EDUCATORS WILL:

13.1. adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure

13.2. ensure they are aware of current child protection law, NSW Child Safe Standards and their duty of care to ensure that reasonable steps are taken to prevent harm to children

13.3. ensure they promote and support a child safe environment, including adherence to the *Child Safe Environment* and *Child Protection* policies and mandatory reporting obligations

13.4. participate in practical training related to digital safety, privacy protection and responsible use of technology

13.5. understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe

13.6. 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

13.7. develop an understanding of the National Model Code and Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 [NSW only] and strictly adhere to these guidelines for taking images or video of children

13.8. not use, or have access to, any personal electronic devices, including mobile phones or smart watches used to take images or video of children at the Service, access social media (Facebook, Instagram or other) whilst working directly with children, unless an exemption has been authorised

13.9. not breach children and families' privacy

13.10.   keep passwords confidential and log out of computers and software programs after each use

13.11.   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

13.12.   ensure children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online

13.13.   introduce concepts to children about online safety at age-appropriate levels

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

P-2.28 Safe Use of Digital Technologies and Online Environments

13.14. support children's understanding of online safety by providing age-appropriate guidance, discussions and activities that help them to recognise safe and unsafe online behaviours

13.15. consult with children about matters that impact them, including the use of digital technologies and online environments, to ensure their voices are heard and respected in a meaningful way

14. FAMILIES WILL:

14.1. adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure

14.2. not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the Service

14.3. provide written authorisation indicating whether or not the Service may take, use, store or destroy images or videos of their child

14.4. provide written notification if they wish to withdraw the authorisation for the Service to take, use, store or destroy images and videos of their child

14.5. 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.)

14.6. be able to withdraw authorisation for the Service to take, use, store or destroy images or videos of children at any time in writing

14.7. be provided with clear information about how to make a complaint and our complaints handling processes

14.8. be aware that sometimes other children in the Service may feature in the same photos, videos, and/or observations as their children. In these cases, families are never to duplicate or upload them to the internet/social networking sites or share them with anyone other than family members

15. VISITORS AND VOLUNTEERS WILL:

15.1. adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the Service

15.2. not use personal electronic devices, such as mobile phones smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the Service

15.3. report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor

15.4. obtain written authorisation from parents/guardians and the approved provider to capture images or video of a child for observation/documentation purposes only. This applies to visitors who are supporting children at the OSHC Service (NDIS funded support professionals, Inclusion Support professionals) (See *ECIP Confidentiality Agreement*).

16. BREACH OF POLICY:

16.1. Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment and may face disciplinary action.

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

16.3. Family members who do not comply with this policy may place their child's enrolment at risk and limit the family members access to the Service.

16.4. Children who breach this policy will face disciplinary action.

17. CONTINUOUS IMPROVEMENT/EVALUATION

17.1. Our *Safe Use of Digital Technologies and Online Environments Policy* will be reviewed on an annual basis in consultation with children, families, staff, educators and management.

RELATED LEGISLATION	
Child Care Subsidy Secretary's Rules 2017	Family Law Act 1975
A New Tax System (Family Assistance) Act 1999	*Privacy Act 1988* (the Act)

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026

Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook in **https://www.education.gov.au/early-childhood/resources/child-care-provider-handbook**

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

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

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.

CHANGE HISTORY	Version	Amendment Details	Date Amended
	New	Newly created policy	Aug 2025

	1	• Policy reviewed due to legislation changes for child safety- National Model Code (NMC) and following the release of the *Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025* mandatory for NSW Services and updated accordingly
		• Minor edits within policy including:
		  ○ added Child Safety and Protection (effective Jan 2026)
		  ○ added 'harmful content' to definitions
		  ○ minor edit to Purpose
		  ○ minor edits – 1.1, 1.2, 1.3
		  ○ added clause 3
		  ○ added 4.1-4.3 and 4.6
		  ○ added clause 5
		  ○ added 11.2.4
		  ○ added 12.6-12.7, 12.11, 12.12, 12.15.4,12.15.5, 12.21,12.24-12.26, 12.32, 12.33, 12.46-12.49
		  ○ added 13.2-13.4, 13.8
		  ○ added 14.3-14.7
		  ○ added 15.4
		• sources checked for currency and updated as required
			Nov 2025

Ref. No.	Issued	Version No.	Supersedes	Approved by	Next Revision Due
P-2.28	Nov 2025	1	NEW	Management Committee	Nov 2026