



SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS PROCEDURE

Every education and care Service is required to have appropriate policies, procedures, risk assessments and authorisations in place to ensure the safe and responsible use of digital technology and online environments by children, educators, staff, visitors, volunteers and families. *Education and Care Services National Regulations* 168(2) (ha), requires the approved provider to ensure that policies and procedures address the safe use of digital technology and online environment, including:

- Clearly outlining how images and videos will be captured, used, stored and destroyed
- Ensuring authorisations include specific details relating to capturing, using, storing and destroying images and videos
- Establishing procedures for all digital devices, including expectations for appropriate use, restricted access and secure data handling
- Implementing procedures for the supervised and age-appropriate use of digital devices by children, including restrictions on device access and internet usage

Our Service adopts and aligns with legislated digital device requirements under the Education and Care Services National Law and Education and Care Services National Regulations and regulator directions (where relevant) for capturing images or videos of children, including the safe storage and retention of images or videos. Our Service will ensure compliance with the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026, ensuring Service-supplied devices are configured to operate in accordance with Service policies and procedures, and that written authorisations are provided where exemptions apply in prescribed circumstances.

Working in conjunction with the *Safe Use of Digital Technologies and Online Environments Policy*, this procedure provides clear guidance to ensure the safe and responsible use of digital devices and online environments by children, families, staff, educators, students and volunteers whilst at the Service. Our

Service ensures all digital technologies and online environments are used in a way where children's safety, rights and best interests are the paramount consideration at all times.

Education and Care Services National Law and Regulations (S.2A, 3A, 162A,162B, 165, 166A, 167.174, Part 6A, R. 12, 73, 76, 84, 115, 122, 123, 149, 155, 156, 168, 170, 171, 172, 175, 176,179A, 179B, 181, 183, 184) NQS QA 2: Element 2.2, 2.1.2 & 2.2.3 Health practices and procedures

Related Policy: Safe Use of Digital Technologies and Online Environments Policy

SAFE USE OF DIGITAL TECHNOLOGY AND ELECTRONIC DEVICES		
The approved provider and nominated supervisor will:		
1	review the Service's <i>Safe Use of Digital Technologies and Online Environments Policy</i> annually in collaboration with educators, staff, families and children	
2	uphold a culture of child safety and wellbeing across all Service operations, ensuring that digital technologies and online learning environments are accessed and used in a manner that safeguards children at all times	
3	implement Part 6A of the Education and Care Services National Law and regulator directions (where relevant) to ensure management, staff, educators, visitors and volunteers are aware of and adhere strictly to the legislative requirements, including: - only Service-supplied or issued devices are to be used when capturing, storing or transferring images or videos of children - personal electronic devices that can capture, store or transfer images or videos (such as tablets, mobile phones, computers/laptops, digital cameras, smart watches, META glasses) and personal storage and file transfer media (such as SD/memory cards, USB drives, hard drives and cloud storage) are not in the possession of any educator, staff member, visitor or volunteer while providing education and care and working directly with children, including during excursions or when children are being transported - ensure educators, staff or volunteers submit a written request if seeking an exemption to use or have in their possession a personal electronic device for essential purposes strict controls are in place for the appropriate storage and retention of images and videos in accordance with our <i>Record Keeping and Retention Policy</i>	
4	Ensure compliance with the Ministerial Direction Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026 including: - maintaining records for all Service-supplied electronic devices - ensuring Service-supplied electronic devices are configured to operate in accordance with Service policies - document the revocation of any electronic devices no longer in use at the Service	

	- providing written authorisation for staff, students or volunteers in prescribed circumstances that may warrant a person to be in possession of or have control of a personal device that can take, store or transfer images or videos while working directly with children - written records and authorisations must be retained for a period of 3 years following the date the record was made	
5	develop and maintain a register of electronic Service-supplied (<i>Electronic Service-supplied Device Form</i>) including: - 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	
6	ensure Service-supplied devices are configured to operate in accordance with Service policies]. See Secure Access to Digital Technologies and Online Environments section below for details.	
7	develop and maintain an <i>Electronic Device Register</i> for all electronic devices purchased and used at the Service. The <i>Electronic Device Register</i> should include type of device, unique identifier (e.g. asset number), who device is allocated to, dates of allocation and return (revocation records).	
8	ensure each electronic device purchased for and used at the Service is clearly marked to state it is the property of the Service	
9	ensure Service-supplied or issued electronic devices are stored securely and are not removed from Service premises (unless for operational activities such as excursions or transportation). Director/Educational Leader and Administration personnel are able to take service devices home for operational activities and must ensure that it is password protected.	
10	advise educators and staff that personal electronic devices can be used on a break provided there are no enrolled children present in the area where the person is using their personal device. Educators and staff must not use personal phones or devices in areas where children are visible.	
11	encourage educators and children to report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes staff/educators/children feel uncomfortable	
12	document and investigate all concerns relating to the safe use of digital technologies or online environments (See: <i>Privacy Law Compliance Procedure</i>)	

13	ensure that screen time for children aged 2 to 5 years does not exceed 1 hour per day	
14	ensure the use of TV, iPads and DVDs is minimised and ensure only age appropriate 'G' rated programs are shown	
15	ensure children only access digital devices, including a computer or mobile device connected to the internet, in open, supervised areas where educators maintain clear line-of-sight	
16	identify and minimise supervision 'blind spots' where technology is used	
17	ensure children are fully supervised and never left unattended whilst using an electronic device, including a computer or mobile device is connected to the internet, including during transport or excursions	
18	ensure children are supported to understand online safety risks, including harmful content, unwanted contact and privacy risks through discussions, programming and prompts where appropriate	
19	support educators to respond appropriately to children who feel unsafe, upset or uncomfortable when using digital technologies	
20	ensure mandatory national child safety training is completed by the approved provider, PMC, management, nominated supervisor, staff, educators, students and volunteers and that prescribed persons refresh child safety training every 2 years	
21	ensure 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	
22	conduct a review of practices following any incident involving digital technologies or online environments, including an assessment of areas for improvement	
23	ensure all incidents, concerns or data or privacy breaches relating to digital technologies are documented and responded to promptly, including notifying the Office of the Australian Information Commissioner (OAIC) by using the online Notifiable Data Breach Form in the event of a data breach	
24	report any concerns related to child safety including inappropriate use of digital technology or inappropriate conduct or breach of child protection legislation to relevant authorities- regulatory authority, police, (<i>see: Child Safe Environment, Child Protection Policies</i>)	
25	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	

STAFF, STUDENT, VOLUNTEER TRAINING AND INDUCTIONS

The approved provider and nominated supervisor will:

1	inform educators and staff of the <i>Safe Use of Digital Technologies and Online Environments Policy and procedures</i> during orientation and induction	
2	keep records of inductions and regular training completed by educators and staff	
3	identify technology training needs of educators for professional development	
4	ensure that educators and staff are aware of current child protection law, National Principles for Child Safe Organisations and duty of care to prevent harm to children	
5	provide regular training for all educators and staff on reporting obligations, including mandatory reporting and child safe practices	
6	provide professional development, information and resources to educators relating to <u>the safe use of digital technologies and online environments</u> from the <i>e-Safety Commissioner- Early Years Program</i>	
7	ensure management, staff, students, visitors and volunteers are aware of and adhere strictly to legislated requirements as described above, including ECIP Professionals	
8	ensure management, staff, students, visitors and volunteers are aware of, and comply with, the Ministerial Direction - Education and Care Services (Supply, Authorisation and Use of Devices) Order 2026 as described above, including ECIP Professionals	
9	inform educators, staff, volunteers and visitors of exemptions 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 including: • 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 essential purposes must be submitted in writing to the approved provider for approval (<i>See Electronic Device Exemption Form</i>) Under no circumstances may a personal device be used to capture, store or transmit images or videos of children, even where an exemption applies • An additional prescribed circumstances may apply if a Service-supplied or issued device stops working and another device is temporarily required • exemptions must be reviewed every 3 months • written prescribed circumstance authorisations must include ○ Service and approved provider details ○ person's details (including name and role) ○ name of the person making authorisation ○ description of personal device	

	○ reasons for the authorisation and ○ duration of the authorisation • exemptions may be revoked as required, with revocation properly documented	
10	Require all staff and educators to complete the following forms to ensure they understand their responsibilities in handling and protecting digital information • <i>Cyber Safety Agreement</i> • <i>East Lismore Community Preschool iPad and Data user agreement</i> • <i>A Statement of Commitment to Child Safety Checklist</i> as part of their induction program • <i>Technology Confidentiality Agreement for Employees and Management Committee</i>	
11	discuss with educators' terms regarding sharing personal data online; ensure children's personal information where children can be identified such as name, address, age, date of birth etc is not shared online	
12	ensure educators are informed of, and adhere to, recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines and the Service's Physical Activity Policy	
13	ensure educators only use educational software programs, websites and apps that have been thoroughly examined for appropriate content prior to allowing their use by children	
14	ensure educators use a search engine such as 'Kiddle' rather than Google to search for images or information with children	
15	ensure staff and educators understand how to identify harmful content, cyberbullying and online abuse	
16	ensure all staff, educators, students and volunteers are aware of their responsibilities and obligations when responding to disclosures of unsafe online experiences	
17	ensure ongoing professional learning for educators and staff includes cyber safety, privacy, and child protection in digital environments	
18	ensure educators and staff are aware of their mandatory reporting requirements and report any concerns related to child safety including inappropriate use of digital technology or inappropriate conduct to the approved provider or nominated supervisor. Reports may be required to be made to the regulatory authority, police, Office of Children's Guardian or e-Safety Commissioner, as required, refer to policy: Identification and reporting of Online Abuse and Safety Concerns for further information.	
19	ensure that all staff and educators comply with Service policies on the safe use of digital technologies, privacy and confidentiality. Staff or educators who fail to comply may face disciplinary action, termination, restricted access or reporting to regulatory or child protection authorities	
20	Inform educators, staff, visitors, volunteers and students that personal devices or storage devices must not be used or in their possession when working directly with children,	

	including tablets or mobile phones, SMART watches that can capture or store images or videos. whilst working directly with children. When Specialists work with our children, they can have a laptop or IPAD to take session notes, however, must not take images or videos of children, and must work within line of sight of other educators. Ensure that all specialists that work with our children complete a <i>Cyber Safety Agreement</i> before working with children.	
--	---	--

FAMILY COMMUNICATION AND ENGAGEMENT		
The approved provider and nominated supervisor will:		
1	inform parents/guardians of the Service's <i>Safe Use of Digital Technologies and Online Environments Policy</i> and procedures upon enrolment	
2	inform families of examples of digital technology and electronic devices used at the Service, which may include: • touchscreen devices- tablets (iPads) • programs that develop literacy or numeracy skills with ICT such as word processing, desktop publishing • internet and information literacy skills • smart toys/robotic toys- such as bee bots • scanners • interactive whiteboards/data projectors	
3	provide parents and families with information about the apps or software programs accessed by children at the Service	
4	ensure families who speak languages other than English understand requirements relating to digital technologies, including authorisations through use of translated documents if required	
5	inform families that personal electronic devices are not to be brought to the Service by children	
6	ensure that personal device's brought to the Service by a child are turned off, securely stored in a locked cupboard, and collected by the child's parent/guardian at the end of the day	
7	ensure families are informed of how complaints regarding digital technologies can be made and how concerns will be managed in line with the <i>Dealing with Complaints Policy</i>	

DIGITAL TECHNOLOGY AND ONLINE ENVIRONMENTS RISK ASSESSMENT		
1	The approved provider and nominated supervisor will conduct a comprehensive risk assessment regarding the safe use of digital technology and online environments by children and staff, identifying potential risks, implementing appropriate controls and ensuring supervision and protective measures are in place	
2	The risk assessment will be developed in consultation with educators, families and, where possible, children	
3	The risk assessment will include assessment of online risks such as harmful content, cyberbullying and inappropriate interactions, as well as risks related to the physical environment, including layout and supervision when using devices, and risks associated with AI tools, software programs, applications and online platforms	
4	Risk assessments will be conducted where the use of personal devices may be used for operational activities such as during excursions or transportation of children where the use of Service-supplied or issued device may not be possible	
5	The approved provider and nominated supervisor will review the risk assessment for safe use of digital technology and online environments is reviewed at least once every 12 months	
6	The approved provider and nominated supervisor will review the risk assessment following any incident or circumstance where the health, safety or wellbeing of children may be compromised	
7	If a risk concerning a child's safety and wellbeing is identified during the risk assessment, the approved provider and nominated supervisor will update the <i>Safe Use of Digital Technologies and Online Environments Policy</i> and procedure as soon as possible	
8	The approved provider and nominated supervisor will ensure the <i>Safe Use of Digital Technologies and Online Environments Risk Assessment</i> is stored safely and securely and kept for a period of 3 years	

SOFTWARE PROGRAMS, APPLICATIONS AND ARTIFICIAL INTELLIGENCE (AI) USE PROCEDURE		
The approved provider and nominated supervisor will:		
1	ensure educators and staff understand the appropriate use of AI tools and software programs in accordance with the <i>Safe Use of Digital Technologies and Online Environments Policy</i>	
2	ensure AI and software tools are only used to support documentation, administrative tasks and planning, and are not used as an authoritative source of information	
3	ensure educators understand how to use AI and software ethically and responsibly. Ensure educators and staff verify all AI-generated content for accuracy, relevance and contextual appropriateness	

4	ensure that sensitive data, including photos, dates of birth and biometric information, is never be uploaded into open-access AI platforms or insecure software programs or applications	
5	ensure that personal or identifiable information about children is not entered into AI platforms or software programs, unless explicitly authorised by families and only where the platform provides clear data storage and deletion policies	
6	ensure transparency with families around AI and software use, including how data is stored, protected and used	
7	ensure all AI and software use complies with privacy, confidentiality and data protection requirements	
SECURE ACCESS TO DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS		
The approved provider and nominated supervisor will:		
1	ensure there is no unauthorised access to the Service's technology facilities (programs, software program etc.)	
2	ensure all educators have appropriate login to provide secure access to programs and folders	
3	inform educators and staff of password management, including any password management system the Service implements. Educators and staff are expected to create strong passwords and to change passwords on a regular basis.	
4	ensure log in and passwords are not shared between staff, families or outside community members to restrict unauthorised access	
5	implement the following measures to protect personal information: • using password protected systems • restricting access to authorised personnel only • storing physical records securely • reviewing data handling practices • providing staff with privacy and data security training	
6	advise new educators or staff of how the Service stores physical and digital files. Educators and staff are provided with Service issued devices, such as USB or Hard Drives to store data information securely if not cloud storage is not used.	
7	ensure monthly backups of data are completed and ensure data is deleted and destroyed in accordance with the <i>Record Keeping and Retention Policy</i>	
8	work with an ICT security specialist to ensure the latest security systems are in place	
9	ensure anti-virus and internet security systems including firewalls can block access to unsuitable web sites, newsgroups and chat rooms	

10	conduct a <i>Privacy Audit</i> to ensure ongoing compliance with privacy obligations and recent changes. The <i>Privacy Audit</i> should be completed on a yearly basis or following any breaches in data at the Service. The <i>Privacy Audit</i> will assist Services to: - Identify how to meet privacy obligations - Identify how to improve on existing privacy management - Identify potential areas of privacy risk - Alleviate these risks by improving compliance with the Privacy Act	
Educators will:		
11	only use approved programs, including online platforms, through authorised accounts and login credentials	
12	manage and maintain password and login details securely in accordance with Service policies, ensuring they are not shared and are updated regularly	
13	attend and participate in privacy and data security training	
14	use Service-supplied devices for the intended use only and not access personal accounts	
IMAGES AND VIDEOS – Capturing, Using, Storing, Destroying and Authorisation		
The approved provider and nominated supervisor will:		
1	engage educators in discussion that consider the intent, appropriateness, context and consent involved in capturing images and videos	
2	ensure images and videos are captured that reflect the intended purpose and are not inappropriate in nature. For example, inappropriate images may include children not dressed adequately, in distress or in a position that could be perceived as sexualised in nature.	
3	ensure educators discuss capturing photos with children and seek their consent in a way that is appropriate to their age and understanding	
4	provide Service-supplied or issued electronic devices to educators and staff for the use of capturing images and videos	
5	provide educators and staff with information and guidelines on how to access, handle, store and transmit digital data securely	
6	ensure staff, educators, students, volunteers or visitors do not transfer images or videos from Service-supplied or issued devices to personal devices or storage devices, unauthorised transferring of digital data may result in disciplinary or other appropriate action	
7	investigate and report any alleged misuse of Service-supplied or issued devices, including where images or videos are not appropriate or have been transferred to personal devices. Reports may be required to be made to the regulatory authority, police, Office of Children’s Guardian or e-	

	Safety Commissioner as required, refer to policy: Identification and reporting of Online Abuse and Safety Concerns for further information.	
8	review all material submitted for publication on the Service Internet/Intranet site and ensure it is appropriate to the Service's learning environment	
9	ensure only authorised persons post images or videos online and that content is appropriate and aligns with the Service's values and objectives	
10	ensure educators or staff seek advice from Service management regarding matters such as the collection and/or display/publication of images or videos (such as personal images of children or adults), as well as text (such as children's personal writing)	
11	inform families of how images and videos of children will be stored	
12	monitor Service-supplied or issued devices to ensure images and videos are captured, used and stored in accordance with the <i>Safe Use of Digital Technologies and Online Environments Policy</i> and this procedure	
13	ensure visitors such as ECIP professionals obtain written authorisation from both the Service and families before capturing images, and ensure external professionals use only Service-supplied or issued devices (or work-issued devices)	
14	store backups securely, either offline, or online (using a cloud-based service), including using password protection systems	
15	regularly update software and devices	
16	establish and implement procedures to be followed in the event of a data security breach (See: <i>Privacy Law Compliance Procedure</i>)	
17	inform families of how images and videos will be destroyed	
18	ensure images and videos are deleted or destroyed once they are no longer required for the purpose for which they were collected, in line with privacy obligations and Service policies	
19	ensure images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian	
20	ensure a confidential record is maintained of children who are not authorised by parents/guardians to be photographed or filmed	
21	ensure authorisation is obtained from parents/guardians to take, use, store and destroy images and videos of children taken at the Service	
22	inform families of the purpose of why educators or staff are capturing photos, i.e. for documenting the education program or child's learning and development or for promotional purposes	
23	request parents/guardians to sign an authorisation form to ensure children's privacy, safety and copyright associated with the online publication of children's personal details, images, videos or	

	work. If authorisation is not provided the child's personal details, images, videos or work will not be published online.	
24	ensure educators and staff do not share images or videos beyond Service-supplied devices or accounts	
25	store backups securely, either offline, or online (using a cloud-based Service), including using password protection systems	

RESIGNATION/EXIT PROCEDURE

1	Educators and staff who provide resignation are informed of their responsibilities and obligations in relation to the <i>Confidentiality Agreement</i>	
2	Management will remove access to email address, SharePoint and/or cloud storage and folders to an educator or staff member who has ended employment	
3	Educators and staff who have resigned are to return any Service issued equipment or devices, including USBs or Hard Drives	
4	Educators and staff who have resigned are to acknowledge not to access accounts or misuse sensitive or confidential information	
5	An <i>Employee Exit Checklist</i> is completed for all educators or staff who have resigned from the Service, in particular attention provided to the Data Security section	
6	Management will consult with the <i>Employee Exit Guide</i> to ensure all aspects of Data Security are considered when an educator or staff member provides resignation	

REVIEW OF PROCEDURE

Date procedure created	30.9.2026	To be reviewed	SEPT 2026
Approved by	Michelle Donadel	Signature	
Procedure Reviewed Date	Modifications/Changes		
November 2025	Procedure updated to support new Ministerial Order Procedure updated following release of the Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 mandatory for NSW Services.		

	Section for Safe use of digital technology and electronic devices has been restructured into 3 separate sections for clarity and ease of navigation.
July 2025	New procedure developed. <i>Data Security Procedure</i> information merged into this procedure.