ECEC Procedure 27.1

Safe use of digital technologies and online environments

Controlled Document

Version:	2.0	**Date of approval:**	March 2026	**Date of next review:**	March 2028
Document Owner:	Manager – Early Childhood and School Aged Education and Care	**Approved by:**	Executive Manager - Children's Services		
Reviewed by:	Project Officer– Early Childhood Education & Care	Quality & Risk			

Policy attached to this procedure	Safe use of digital technologies and online environments

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 taken, used, stored and destroyed
- Ensuring authorisations include specific transportation details
- Informing families and staff about the use of any optical surveillance devices through clear signage and communication, and ensuring all devices comply with applicable state/territory and federal privacy legislation
- 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 the National Model Code and Guidelines for taking 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 2025, 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.

Education and Care Services National Law or Regulations (S. 162A, 165, 166A, 167. R. 12, 73, 76, 84, 115, 122, 123, 149, 155, 156, 168, 170, 171, 172, 175, 176, 181, 183, 184) NQS QA 2: Element 2.2, 2.1.2 & 2.2.3 Health practices and procedures

STAFF PROCEDURE: SMARTWATCHES AND PERSONAL ELECTRONIC DEVICES		
To maintain a child safe environment and protect the privacy of children and families, the following staff procedures apply:		
1	Only service-issued electronic devices may be used for documenting children's learning, taking photographs, recording videos, or communicating with families. These devices must be used in accordance with the service's documentation, privacy and child safety policies and procedures.	
2	Educators, staff, students and volunteers must store personal electronic devices, including mobile phones and smart watches, in a designated staff area, locker or secure storage while working directly with children.	
3	Personal electronic devices may only be accessed during scheduled breaks and in staff-only areas, away from children.	
4	Staff must not wear smartwatches while working directly with children, regardless of the device capabilities.	
5	The approved provider and nominated supervisor will 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 (See *Electronic Device Exemption Form*) Additional exemptions for NSW Services include: • 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 o Service details, o person's details,	

	○ reasons for the authorisation and ○ duration of the authorisation • exemptions must be reviewed every 3 months exemptions may be revoked as required, with revocation properly documented	
6	The Nominated Supervisor or Responsible Person will monitor compliance with this procedure as part of regular supervision and workplace practices.	

SAFE USE OF DIGITAL TECHNOLOGY AND ELECTRONIC DEVICES		
The approved provider and nominated supervisor will:		
1	review the Service's *Safe Use of Digital Technologies and Online Environments Policy* annually in collaboration with educators, staff, families and children	
2	implement the https://www.acecqa.gov.au/national-model-code-taking-images-early-childhood-education-and-care National Model Code and Guidelines and ensure management, staff and educators, visitors and volunteers are aware of and adhere strictly to the guidelines, including: • only Service-supplied or issued devices are to be used when taking, storing or transferring images or videos of children • personal electronic devices that can take, 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 *Record Keeping and Retention Policy*	
3	ensure compliance with the Ministerial Direction Education and Care Services (Supply, Authorisation and Use of Devices) Order 2025 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	
4	CatholicCare IT department will develop and maintain records of electronic Service-supplied devices 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	
5	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.	
6	develop and maintain an *Electronic Device Register* for all electronic devices purchased and used at the Service (CatholicCare IT)	
7	ensure each electronic device purchased for and used at the Service is clearly marked with an identification code and marked to state it is the property of the Service	
8	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)	
9	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	
10	document and investigate all concerns relating to the safe use of digital technologies or online environments	
11	Adhere to screen time limits: • children birth to one year do not spend any time in front of a screen • children 2 to 5 years of age are limited to less than one hour per day • children aged 5-12 years screen time does not exceed 2 hours per day	
12	ensure the use of TV, iPads and DVDs is minimised and ensure only age appropriate 'G' rated programs are shown	
13	Where schools assign homework in a digital format, children may use their personal iPad or tablet, a school-issued device or a CatholicCare device. Device use for homework will only occur during designated homework periods and must be under the direct and continuous supervision of educators to ensure appropriate and responsible use.	

14	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.	
15	inform families that personal electronic devices, with the exception of point 13 (homework) above, are not to be used at the Service by children. This includes mobile phones and smartwatches. All mobile phones and smart watches must remain switched off and stored in the child's school bag at all times while attending the service.	
16	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	
17	conduct a review of practices following any incident involving digital technologies or online environments, including an assessment of areas for improvement	
18	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, (*see: Child Safeguarding Policies)*	
19	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	

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 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	
4	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	
5	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 *Safe Use of Digital Technologies and Online Environments Policy* and procedure as soon as possible	

6	The approved provider and nominated supervisor will ensure the *Safe Use of Digital Technologies and Online Environments Risk Assessment* is stored safely and securely and kept for a period of 3 years	

IMAGES AND VIDEOS – Taking, 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 taken 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 taking 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 taking 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 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 when required, 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	ensure educators and staff do not share images or videos beyond Service issued devices or accounts	

13	monitor Service issued devices to ensure images and videos are taken, used and stored in accordance with the *Safe Use of Digital Technologies and Online Environments Policy* and this procedure	
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 *Information & Communication Technology – Security Policy)*	
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 authorisation is obtained from parents/guardians to take, use, store and destroy images and videos of children taken at the Service	
21	inform families of the purpose of educators or staff taking photos, ie for documenting the education program or child's learning and development or for promotional purposes	

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 information on privacy and data security	

6	ensure each person who is responsible for submitting data to CCSS through Xplor will be registered with PRODA	
7	ensure all provider personnel using Xplor will have their details updated and background checks conducted as required - [personal details, date of birth, address, email, phone number, Working with Children's Check, Supporting Documentation-Australian Police Criminal History Check, declaration- Australian Securities and Investments Commission (ASIC), National Personal Insolvency Index check]	
8	advise new educators or staff of how the Service stores physical and digital files.	
9	work with CatholicCare's IT department to ensure the latest security systems are in place	
10	ensure anti-virus and internet security systems including firewalls can block access to unsuitable web sites, newsgroups and chat rooms	
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	comply with the CatholicCare AI Usage and Integration Policy and must not enter identifying information related to children, families, or staff.	

RESIGNATION/EXIT PROCEDURE		
1	Educators and staff who provide resignation are informed of their responsibilities and obligations in relation to the code of ethics and conduct agreement	
2	CatholicCare's IT Department 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	
4	Educators and staff who have resigned are to acknowledge not to access accounts or misuse sensitive or confidential information	
5	An Employee Exit Checklist is completed for all educators or staff who have resigned from the Service, in particular attention provided to the Data Security section	