ECEC Procedure 27.1

Safe use of digital technologies and online environments

Controlled Document

Version:	1.0	**Date of approval:**	02/09/2025	**Date of next review:**	02/09/2028
Document Owner:	Project Officer– Early Childhood Education & Care	**Approved by:**	Manager – Early Childhood Education & Care		
Reviewed by:	Administration Assistant – 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

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

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	inform parents/guardians of the Service's *Safe Use of Digital Technologies and Online Environments Policy* and procedures upon enrolment	
3	inform educators and staff of the *Safe Use of Digital Technologies and Online Environments Policy and procedures* during orientation and induction	
4	keep records of inductions and regular training completed by educators and staff	
5	identify technology training needs of educators for professional development	
6	provide regular training for all educators and staff on reporting obligations, including mandatory reporting and child safe practices	
7	provide professional development, information and resources to educators relating to the safe use of digital technologies and online environments from the *e-Safety Commissioner- Early Years Program*	
8	implement the National Model Code and Guidelines and ensure management, staff and educators adhere to these recommendations for taking images or video of children	
9	require new staff and educators to complete a *Cyber Safety Agreement* as part of their induction program to ensure they understand their responsibilities in handling and protecting digital information	
10	inform educators, staff, volunteers and students that personal devices or storage devices must not be used or in their possession when working directly with children, including tablets, mobile phones or smart watches that can capture images or videos	
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	inform families of examples of digital technology and electronic devices used at the Service, which may include: • touchscreen devices- tablets (iPads) • smart boards • televisions	
13	maintain an Electronic Device Register for all electronic devices purchased and used at the Service (IT department)	
14	inform families that personal electronic devices are not to be used at the Service by children (smart watches/mobile phones)	

15	ensure that personal device's brought to the Service by a child are turned off, securely stored, and collected by the child's parent/guardian at the end of the day	
16	ensure educators are informed of, and adhere to, recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines	
17	ensure that children aged 0-1 year do not spend any time in front of a screen	
18	ensure that screen time for children aged 2 to 5 years does not exceed 1 hour per day	
19	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	
20	ensure educators only use software programs, websites and apps that have been thoroughly examined for appropriate content prior to allowing their use by children	
21	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	
22	document and investigate all concerns relating to the safe use of digital technologies or online environments	
23	conduct a review of practices following any incident involving digital technologies or online environments, including an assessment of areas for improvement	
24	report any breach of child protection legislation to relevant authorities, police, Communities and Justice (*see: Child Safeguarding Policies)*	
25	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	

DIGITIAL 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	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 include: • Emergency communication during incidents such as a lost child, injury, lockdown, or evacuation • Personal health needs requiring device use (e.g. heart or blood sugar monitoring) • Disability related communication needs • Urgent family matters (e.g. critically ill or dying family member) • Local emergency event to receive alerts (e.g. government bushfire or evacuation notifications)	
4	ensure educators discuss taking photos with children and seek their consent in a way that is appropriate to their age and understanding	
5	provide Service issued electronic devices to educators and staff for the use of taking images and videos	
6	provide educators and staff with information and guidelines on how to access, handle, store and transmit digital data securely	
7	ensure staff or educators do not transfer images or videos from Service issued devices to personal devices or storage devices, unauthorised transferring of digital data may result in disciplinary action	
8	investigate any alleged misuse of Service issued devices, including where images or videos are not appropriate or have been transferred to personal devices	
9	review all material submitted for publication on the Service Internet/Intranet site and ensure it is appropriate to the Service's learning environment	
10	ensure only authorised persons post images or videos online and that content is appropriate and aligns with the Service's values and objectives	

11	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)	
12	inform families of how images and videos of children will be stored	
13	ensure educators and staff do not share images or videos beyond Service issued devices or accounts	
14	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	
15	store backups securely, either offline, or online (using a cloud-based service), including using password protection systems	
16	regularly update software and devices	
17	establish and implement procedures to be followed in the event of a data security breach (See *Information & Communication Technology – Security Policy)*	
18	inform families of how images and videos will be destroyed	
19	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	
20	ensure images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian	
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 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 ICT 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:		
12	only use approved programs, including online platforms, through authorised accounts and login credentials	
13	manage and maintain password and login details securely in accordance with Service policies, ensuring they are not shared and are updated regularly	

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 ICT 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	