ECEC Policy 27

Safe use of digital technologies and online environments

Approval rating 4

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 and consulted with:		Administration Assistant – Early Childhood Education & Care		Quality & Risk IT Systems Officer	

Statement

Our Service is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, families and community. As a child safe organisation, our Service embeds the National Principles for Child Safe Organisations 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.

Purpose

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

Scope

This policy applies to children, families, staff, educators, management, approved provider, nominated supervisor, volunteers, students and visitors of the Service.

TERMINOLOGY	
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
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.

Source: Glossary to NQF Child Safe Culture and Online Safety Guides- ACECQA 2025

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.

In the OSHC environment it is also important to have a school/leisure balance which means allowing time for play and leisure activities (My Time, Our Place). To achieve this, our OSHC Service may offer children opportunities to use age-appropriate and non-violent video games and/or gaming apps under the supervision of educators.

Children's personal devices – mobile phones, tablets, wearable technology

Parents will be asked to provide permission for their child to use their own device at OSHC and to acknowledge our Cyber Safety Agreement.

We recognise that many children have wearable devices ie. Smart watches. These devices have features which could include accessing internet, taking photos, videos or recording. Children who own a wearable device will be asked to keep it in aeroplane mode for the duration of the session.

Digital technology and electronic devices used at the service

Our Service follows the National Model Code and Guidelines for taking images or videos of children.

The approved provider will inform staff, educators, visitors, volunteers and family members that the use of personal electronic devices used to take photos, record audio or capture video of children who are being educated and cared for at the Service is strictly prohibited. This includes items such as tablets, phones, digital cameras, smart watches, META sunglasses and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage). These devices should not be in the possession of staff, educators or visitors (e.g. ECIP professionals) while working directly with children.

Staff and educators are advised that electronic devices belonging to 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 for operational activities, for example excursions or transportation.

The approved provider will inform staff, educators 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. Staff, educators or visitors with an exemption must not use the personal device to take images or videos of children. Exemptions need to be provided for in writing by the approved provider and may 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)

CatholicCare's ICT department will maintain an asset register of electronic devices purchased by the agency and used at each service. The Asset Register contains sufficient information to enable positive identification of assets. The following details are recorded against each asset:

- a unique asset number/code
- date of acquisition
- cost/purchase price
- description
- location

In services where schools assign homework in digital format, students are permitted to use personal devices, school-issued devices, or CatholicCare devices during designated homework periods. All device usage must occur under the direct and continuous supervision of educational staff to ensure appropriate and responsible use. Children will not be permitted to use their own mobile phone devices in the service. These are to remain in the child's school bag at all times.

Images and videos

The approved provider is responsible for determining who is authorised to take, use, store and destroy images and videos of children using Service 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 Service 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.

CatholicCare systems and servers are backed up and backups are retained as defined by regulatory requirements. Digital data stored at the Service will be destroyed in accordance with the Record Keeping and Retention Policy and procedure. Digital data on Xplor (Childcare Management System) is securely stored in line with Xplor's Privacy Notice.

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.

Physical environment and active supervision

The approved provider, nominated supervisor, management and educators will:

- ensure children are always supervised and never left unattended whilst an electronic device is connected to the internet
- 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
- reflect on our Service's physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology

- perform regular audits to identify risks to children's safety and changes in room set-ups that can indicate areas of higher-risk and become supervision 'blind spots'
- ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members when working with children
- only permit children to use devices in open areas where educators can monitor children's use
- be aware of high-risk behaviours for children online, including uploading private information or images, engaging with inappropriate content (inadvertently or purposefully), making in-app purchases, and interacting with unsafe individuals
- ensure all visitors and volunteers are supervised at all times
- ensure all devices are password protected with access for staff only

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

Software programs and apps

Our Service uses a range of secure software programs and apps on Service-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.

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. Xplor is used by educators to share observations, photos, videos, daily reports, and learning portfolios with families in a secure, closed platform. In addition, Xplor also assists in managing the Service's financial, staffing, and operational requirements.

Artificial intelligence (AI) interactions and guidelines

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.

Confidentiality and privacy guidelines

Our Privacy 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.

The approved provider will immediately notify CatholicCare's IT department in the event of a possible data breach. This could include:

- a device containing personal information about children and/or families is lost or stolen (parent names and phone numbers, dates of birth, allergies, parent phone numbers)
- a data base with personal information about children and/or families is hacked
- personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)
- this applies to any possible breach within the Service or if the device is left behind whilst on an excursion
- ensure educators are aware of their mandatory reporting requirements and report any concerns

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

Identification and reporting of online abuse and safety concerns

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

The approved provider, nominated supervisor and management will:

- 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 Safeguarding policies*]
- 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 Safeguarding Policies, Behaviour Guidance Policy* and reporting procedures

  - respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management
- ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required
- 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
- 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.

The approved provider/nominated supervisor/management will ensure:

- that obligations under the *Education and Care Services National Law and National Regulations* are met
- educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure
- new employees, students and volunteers are provided with a copy of the *Safe Use of Digital Technologies and Online Environments Policy* and procedure as part of their induction and are advised on how and where the policy can be accessed
- all staff, educators, volunteers and students are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children
- 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
- they promote and support a child safe environment, ensuring adherence to the *Child Safeguarding* policies, including mandatory reporting obligations
- the National Principles for Child Safe Organisations is embedded into the organisational structure and operations
- professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments
- develop and monitor an *Asset Register* for all electronic devices purchased and used at the Service
- appropriate ratios and adequate supervision are maintained for children at all times including when using digital technology and accessing online environments
- students, volunteers and/or visitors are never left alone with a child whilst at the Service under any circumstances

- 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:
    - 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
    - staff and educators only use electronic devices issued by the Service for taking images or videos of children enrolled at the Service
    - Service issued devices are securely configured, monitored and maintained to prevent unauthorised access
    - visitors who are supporting children at the 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.
- 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: *Client and Stakeholder Feedback - includes Compliments and Complaints)*
- the *Privacy Policy* is adhered to at all times by staff, educators, families, visitors, volunteers and students
- 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
- written authorisation is requested from families to take, use, store and destroy digital documentation including images and videos of children
- images or videos of children are not taken, used or stored without prior parent/guardian authorisation
- written authorisation is obtained from parents/guardians for children to use electronic devices
- written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (Website, Facebook, Instagram or Xplor).
- families are informed to withdraw authorisation, a written request is required
- images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian
- 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
- digital data is stored securely according to CatholicCare's Privacy Policy

- 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
- they remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the Office of the Australian Information Commissioner (OAIC)
- a risk assessment is conducted regarding the use of digital technologies by staff and children at the Service, including accessing online environments
- 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
- 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
- staff, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies and online environments
- a review of practices is conducted following an incident involving digital technologies or online environments, including an assessment of areas for improvement
- to install and maintain anti-virus and internet security systems including firewalls to block access to unsuitable web sites, newsgroups and chat rooms
- educators are informed of, and adhere to recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines:
    - children birth to one year should not spend any time in front of a screen
    - children 2 to 5 years of age should be limited to less than one hour per day
    - children 5-12 years of age should limit screen time for entertainment to no more than 2 hours a day.
- they share information to families about recommended screen time limits based on Australia's Physical Activity and Sedentary Behaviour Guidelines.

Educators will:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
- ensure they are aware of current child protection law, National Principles for Child Safe Organisations and their duty of care to ensure that reasonable steps are taken to prevent harm to children

- ensure they promote and support a child safe environment, ensuring adherence to the *Child Safeguarding Policies,* including mandatory reporting obligations
- participate in practical training related to digital safety, privacy protection and responsible use of technology
- understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe
- promote and contribute to a culture of child safety and wellbeing in all aspects of our Service's operations, including when accessing digital technologies and online learning environments
- not use, or have access to, any personal electronic devices, including mobile phones or smart watches used to take images or video of children at the Service, access social media (Facebook, Instagram or other) or breach children and families' privacy
- keep passwords confidential and log out of computers and software programs after each use
- 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
- ensure children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online
- ensure that screen time is NOT used as a reward or to manage challenging behaviours under any circumstances
- introduce concepts to children about online safety at age-appropriate levels
- 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
- 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.

Families will:

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

Visitors and volunteers will:

- adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the Service
- 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
- report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor
- obtain written authorisation from parents/guardians to capture images or video of a child for observation/documentation purposes only. This applies to visitors who are supporting children at the Service (NDIS funded support professionals, Inclusion Support professionals).

Consequences of Policy Violations:

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. The severity of the consequences will depend on the nature and impact of the violation, as determined by CatholicCare Wollongong. People and Culture will review each case individually to determine appropriate actions based on the circumstances.

Related Policies

IT Acceptable Use and Security Policy Information & Communication Technology – Security Policy Child Safeguarding Policies Code of Conduct Client and Stakeholder Feedback Educational Program Policy Enrolment Policy	Governance and Leadership Policy Fraud Prevention Policy Incident, Injury, Trauma, and Illness Policy Interactions with Children Families and Staff Policy Photograph Policy CatholicCare Privacy Policy Record Keeping and Retention Policy Student, Volunteer and Visitor Policy

Related Resources

- Cyber Safety Agreement
- Safe Use of Digital Technologies and Online Environment Procedure
- Information & Communication Technology - Security Procedure
- Australian Children's Education & Care Quality Authority. National Model for Early Childhood Education and Care.
- Australian Government Office of the eSafety commission
- eSafety Early Years Program for educators
- eSafety Early Years Program checklist
- eSmart Alannah & Madeline foundation
- Family Tech Agreement. eSafety Early Years Online safety for under 5s

- Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content: https://www.kiddle.co/
- Office of the Australian Information Commissioner (OAIC)

Key Resources

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2	Safety	Each child is protected
2.2.1	Supervision	At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.
2.2.3	Child Safety and Protection (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 7: 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.

Relevant Legislation

EDUCATION AND CARE SERVICES NATIONAL LAW AND NATIONAL REGULATIONS	
S. 162A	Child protection training
S. 165	Offence to inadequately supervise children
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 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)
Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook	

Induction and ongoing training

Induction and ongoing training will be implemented, focusing on this policy and related procedures.

Information will be shared with relief/ casual educators on induction and as relevant to the environments that they are working in, their shift responsibilities and the children in their care.

Sources

Australian Children's Education & Care Quality Authority. (2025). https://www.acecqa.gov.au/sites/default/files/2023-03/Guide-to-the-NQF-March-2023.pdf*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. (2025). https://www.acecqa.gov.au/sites/default/files/2023-03/Guide-to-the-NQF-March-2023.pdf*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.
Western Australian Legislation Education and Care Services National Law (WA) Act 2012
Western Australian Legislation Education and Care Services National Regulations (WA) Act 2012

Policy created/ Reviewed

Date	Major, Minor or Administrative	Description of Revision(s)
August 2025	Major	New policy

Monitoring, Evaluation and Review

This policy will be reviewed periodically to ensure its effectiveness and relevance. Any necessary updates or modifications to ensure compliance with legislative and standard requirements will be communicated to all employees, contractors, and representatives of CatholicCare Wollongong.

Other situations may include:

- Following an incident, to identify gaps and strengthen data protection measures.
- adoption of new tools or systems.
- mergers, restructuring, or shifts in services that impact on current processes.
- As part of routine evaluations to ensure policies remain effective and aligned with best practices.
- If client/s provide feedback or complaints, prompting a review for improvement.
- When inefficiencies or errors are identified.

The agency will formally review this Policy every three years as part of the policy's known life cycle period.

	Type of Policy

Approval rating 1	New agency policy/adjustments that are legislated or are a Diocesan directive. Minimal collaboration required.
Approval rating 2	High level agency policies that are developed at executive management level (such as employee entitlements) go to CELT for final review before COO recommendation for approval by the CEO.
Approval rating 3	Operational agency policies are endorsed by the QSC to ensure policy is applicable across all program areas. Then go to CELT for final review before COO recommendation for approval by the CEO.
Approval rating 4	Program specific where it is only the individual program that need to ensure that the policy meets practice requirements. No QSC, CELT or CEO. However, if it is a new policy, courtesy email outlining what they are should go to the CEO, COO and EM Quality & Risk (EM Q&R) for information only.