Safe Use of Digital Technologies and Online Environments Policy

Policy Number:	12.26
Policy Category:	Childcare Centre
Authorised by:	Res-2025-08-233
Date approved:	14/08/2025
Review Date:	14/08/2026

Longreach Regional Council
Ilfracombe Isisford Longreach Yaraka

OBJECTIVE

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.

SCOPE

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

LEGISLATION

Education and Care Services National Law Act 2010. (Amended 2024)
Education and Care Services National Regulations. (Amended 2025)
Child Care Subsidy Secretary's Rules 2017
A New Tax System (Family Assistance) Act 1999
Privacy Act 1988 (the Act)
Family Law Act 1975
Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook

DEFINITIONS

Department of Education - Early Childhood Education and Care (ECEC) – Regulatory Authority responsible for the approval, monitoring and quality assessment of services in their jurisdiction in accordance with the national legislative framework and in relation to the National Quality Standard.

Educator – early childhood or school age practitioner who works directly with children in early childhood or school age care settings.

National Quality Framework (NQF) – provides a national approach to regulation, assessment and quality improvement for early childhood education and care and outside school hours care services across Australia.

National Quality Standard (NQS) – sets a high national benchmark for early childhood education and care and outside school hours care services in Australia. The NQS includes seven quality areas that are important outcomes for children. Services are assessed and rated by their regulatory authority against the NQS, and given a rating for each of the 7 quality areas and an overall rating based on these results.

Parents/Guardians – a person who has parental responsibility for the child.

Staff – employee of Longreach Regional Council based at the Longreach Childcare Centre.

Approved Provider – Longreach Regional Council

Nominated Supervisor – a person with responsibility for the day to day management of an approved service.

Leadership Team – an internal group of leaders within the Childcare Centre comprising of the Childcare Services Director, the Childcare Services Assistant Director and the Staff Engagement and Development Officer.

OWNA – the digital platform utilised by the Longreach Childcare Services for the recording of information.

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.

POLICY STATEMENT

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.

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.

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:

1) Emergency communication during incidents such as a lost child, injury, lockdown, or evacuation
2) Personal health needs requiring device use (e.g. heart or blood sugar monitoring)
3) Disability related communication needs
4) Urgent family matters (e.g. critically ill or dying family member)
5) Local emergency event to receive alerts (e.g. government bushfire or evacuation notifications)

Our Service Provider will develop and maintain a register of all electronic devices purchased for and used within the Service. This register will include details such as the device type, date of purchase, intended use, assigned user (if applicable), security settings, and any features related to connectivity, data storage, or recording capabilities. Devices recorded in the register may include, but are not limited to, computers, tablets, mobile phones, cameras, CCTV systems, audio recorders, smart toys, baby monitors and any other internet-connected or data-enabled devices used within the Service.

Children enrolled at our Service are not permitted to bring electronic devices to the Service unless an exception has been discussed with the approved provider or nominated supervisor where the device may be required to support a diagnosed medical condition or disability. If a child brings an electronic device to the Service, it will be switched off and stored in a locked cupboard.

Images and Videos

The approved provider and/or nominated supervisor 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.

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

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

1) ensure children are always supervised and never left unattended whilst an electronic device is connected to the internet
2) provide a child safe environment to children- reminding them if they encounter anything unexpected that makes them feel uncomfortable, scared or upset, they can seek support from staff
3) reflect on our Service's physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology
    - 3.1 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'
    - 3.2 ensure location of digital technology/equipment allows educators to remain in line-of-sight of other staff members when working with children

3.3 only permit children to use devices in open areas where educators can monitor children's use
3.4 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
3.5 ensure all visitors and volunteers are supervised at all times
3.6 ensure all devices are password protected with access for staff only

4) 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. Our educational program software is used by educators to share observations, photos, videos, daily reports, and learning portfolios with families in a secure, closed platform.

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

Confidential and Privacy Guidelines

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

The approved provider will notify the Office of the Australian Information Commissioner (OAIC) in the event of a possible data breach by using the online Notifiable Data Breach Form. This could include:

1) a device containing personal information about children and/or families is lost or stolen (parent names and phone numbers, dates of birth, allergies, parent phone numbers)
2) a data base with personal information about children and/or families is hacked

3) personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)
4) this applies to any possible breach within the Service or if the device is left behind whilst on an excursion
5) 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:

1) ensure all staff, educators, students and volunteers are aware of their mandatory reporting obligations and promptly report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor [See *Child Protection Policy*]
2) support educators to:
    2.1 encourage children to seek support if they encounter anything unexpected that makes them feel uncomfortable, scared or upset
    2.2 listen sensitively and respond appropriately to any disclosures children may make relating to unsafe online interactions or exposure to inappropriate content, adhering to the *Child Protection Policy, Behaviour Guidance: Bullying Policy* and reporting procedures
    2.3 respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management
3) ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required
4) 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
5) 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:

1) that obligations under the *Education and Care Services National Law and National Regulations* are met
2) educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure
3) 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
4) 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
5) 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
6) they promote and support a child safe environment, ensuring adherence to the *Child Safe Environment and Child Protection Policies,* including mandatory reporting obligations

7) the National Principles for Child Safe Organisations is embedded into the organisational structure and operations
8) professional learning is provided to educators and staff relating to the safe use of digital technologies and online environments
9) develop and monitor an *Electronic Device Register* for all electronic devices purchased and used at the Service
10) appropriate ratios and adequate supervision are maintained for children at all times including when using digital technology and accessing online environments
11) students, volunteers and/or visitors are never left alone with a child whilst at the Service under any circumstances
12) all staff, educators, volunteers and students are aware of the National Model Code and Guidelines and adhere to these recommendations for taking images or video of children including:
    - 12.1 personal electronic devices or personal storage devices, that can take images or videos, are not used by educators, staff, visitors or volunteers when working directly with children
    - 12.2 staff and educators only use electronic devices issued by the Service for taking images or videos of children enrolled at the Service
    - 12.3 Service issued devices are securely configured, monitored and maintained to prevent unauthorised access
    - 12.4 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.
13) children, educators and parents are aware of our Service's complaints handling process to raise any concerns they may have about the use of digital technologies or any other matter (see: *Dealing with Complaints Policy*)
14) the Service *Privacy and Confidentiality Policy* is adhered to at all times by staff, educators, families, visitors, volunteers and students
15) 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
16) written authorisation is requested from families to take, use, store and destroy digital documentation including images and videos of children
17) images or videos of children are not taken, used or stored without prior parent/guardian authorisation
18) written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (Website, Facebook and OWNA)
19) families are informed to withdraw authorisation, a written request is required
20) images and videos for individual children are deleted or destroyed and removed from storage when authorisation has been revoked from the parent/guardian
21) 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
22) digital data is stored securely, whether offline or online, using a cloud-based service, and that data is archived regularly
23) 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
24) external agencies or specialists are consulted if concerns are identified relating to online abuse, cyberbullying or digital safety risks

25) policies and procedures reflect a commitment to equity and diversity, protect children's privacy, and empower children to be independent
26) collaboration with relevant professionals, as required, to support equitable access to digital technologies for all children
27) they remain informed of privacy legislation through monitoring of updated from relevant government authorities such as the Office of the Australian Information Commissioner (OAIC)
28) a risk assessment is conducted regarding the use of digital technologies by staff and children at the Service, including accessing online environments
29) 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
30) 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
31) staff, educators, families and children are informed of updates to policies, procedures or legislation relating to digital technologies and online environments
32) a review of practices is conducted following an incident involving digital technologies or online environments, including an assessment of areas for improvement
33) to install and maintain anti-virus and internet security systems including firewalls to block access to unsuitable web sites, newsgroups and chat rooms
34) educators are informed of, and adhere to recommended timeframes for 'screen time' according to Australia's Physical Activity and Sedentary Behaviour Guidelines:
    - 35.1 children birth to one year should not spend any time in front of a screen
    - 35.2 children 2 to 5 years of age should be limited to less than one hour per day
    - 35.3 children 5-12 years of age should limit screen time for entertainment to no more than 2 hours a day.

Educators Will:

1) adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
2) 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
3) ensure they promote and support a child safe environment, ensuring adherence to the *Child Safe Environment* and *Child Protection Policies,* including mandatory reporting obligations
4) participate in practical training related to digital safety, privacy protection and responsible use of technology
5) understand the critical importance of implementing active supervision strategies when children are accessing online environments to keep children safe
6) promote and contribute to a culture of child safety and wellbeing in all aspects of our Service's operations, including when accessing digital technologies and online learning environments
7) 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
8) keep passwords confidential and log out of computers and software programs after each use
9) 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
10) ensure children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online
11) ensure that screen time is NOT used as a reward or to manage challenging behaviours under any circumstances

12) introduce concepts to children about online safety at age-appropriate levels
13) 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
14) 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.

Parents/Guardians Will:

1) adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure
2) not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the Service
3) 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:

1) adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the Service
2) not use personal electronic devices, such as mobile phones smart watches or META sunglasses, to take photos, record audio, or capture video of children being educated and cared for at the Service
3) report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor
4) 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)

Breach Of Policy

Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment and may face disciplinary action. Visitors or volunteers who fail to comply to this policy may face termination of their engagement. Family members who do not comply with this policy may place their child's enrolment at risk and limit the family members access to the Service.

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Safe Use of Digital Technologies and Online Environments Policy* will be reviewed on a regular basis in consultation with children, families, staff, educators and management. Families will be notified of changes to policies within 14 days to ensure they remain informed and can provide feedback or ask questions as needed.

RELATED RESOURCES

Related Policies	Related Documents
Behaviour Guidance: Bullying Policy	Electronic Device Register
CCS Data Security Policy	Media Authorisation Child
CCS Personnel Policy	Media Authorisation Staff
CCS Governance Policy	Privacy Audit
Child Safe Environment Policy	Privacy and Confidentiality Procedure
Child Protection Policy	

Code of Conduct Policy Fraud Prevention Policy Incident, Injury, Trauma, and Illness Policy Interactions with Children Families and Staff Policy Photography Policy Privacy and Confidentiality Policy Programming Policy	Safe Use of Digital Technologies and Online Environment Procedure CCS Compliance Checklist and Audit Cyber Safety Agreement Cyber Safety Authorisation Data Breach Response Record Data Security Checklist Digital Technologies Risk Assessment ECIP Confidentiality Agreement

Authorised by resolution as at 14/08/2025:

_____

Brett Walsh
Chief Executive Officer