

Document Name	Document Version Number	Review Date
Children Services Safe Use of Digital Technologies and Online Environments Policy Family Day Care	1.0.0	February 2027
Date Adopted	Minute Number	Status
18 February 2026	7050	New Policy

Purpose

Council's Family Day Care (FDC) Service is committed to fostering a culture that creates and maintains a safe online environment with support and collaboration from staff, Family Day Care (FDC) educators, families and community.

As a Child Safe organisation, our FDC 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, FDC educators, relief educators, management, approved provider, nominated supervisor, students, volunteers and visitors of the FDC Service.

Definitions

Artificial intelligence (AI):	An engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set 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 abused, 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 crime 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
Service Issued Device:	Any device that is only used for providing education and care (and not personal use) and is registered with Greater Hume Children Services
Registered Device:	a register of all electronic devices purchased for and used for the provision of the FDC Service and approved residences/venues

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

Policy Content

Greater Hume Children Services FDC staff and educators use 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 and CCTV monitoring.

This policy and all relevant associated documents are in line with Child Safe Standards. As a Child-safe organisation we are committed to creating and maintaining a child safe culture, and we will diligently review and adapt both physical and online environments to minimise the risks of abuse. We will actively engage with families and communities to support children in all areas of their safety and wellbeing.

NSW Educators

NSW registered Educators may use personal electronic devices to take images, record audio or capture video of children, with additional security protections applied, for the purpose of providing family day care and the device is registered with the approved provider. Educators will follow strict guidelines set out by Greater Hume Children Services to ensure the safety and privacy of all children in care is protected.

Victorian Educators

Victorian Registered Educators can only use service-issued devices (*and not personal use*) to take images, record audio or capture video of children, with additional security protections applied, for the purpose of providing family day care and the device is registered with the approved provider. Educators will follow strict guidelines set out by Greater Hume Children Services to ensure the safety and privacy of all children in care is protected. (*This is considered a 'service-issued' device*)

All Educators

Greater Hume Children Services Family Day Care will develop and maintain a register of all electronic devices purchased for and used for the provision of the FDC Service and approved residences/venues. 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 FDC Service.

Children enrolled with Greater Hume Children Services Family Day Care are not permitted to bring electronic devices to the FDC Service residence or approved venue, unless an exception has been discussed with the approved provider and FDC educator where the device may be required to support a diagnosed medical condition or disability or for school issued homework. The device must not contain or be able to access any inappropriate material. If a child brings an electronic device to the FDC Service, it will be switched off and stored in a locked cupboard, out of reach of children.

Images and Videos

Images and videos of children must only be taken and used in accordance with FDC Service policies, and careful consideration given to the purpose of the image or video. FDC educators and staff 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.

Educators will ensure all parent permissions have been obtained before any images or videos are taken.

Storage

Images and videos of children must be stored with stringent protections to limit access exclusively to educators and authorised personnel. This requirement extends to all service issued device and personal storage media devices, includes phones, computers, SD cards, USB drives, hard drives and cloud-based applications that can store images and video recordings. Additionally, care must be taken during the transfer of media from one device to another to ensure security and confidentiality.

As soon as images and videos have been used for their purpose – e.g. the program or for sharing with a parent, they must be deleted from all personal devices and service issued devices.

Educator family, household members, enrolled children's family members and authorised nominees, and visitors to the service

The taking of images or videos of children in care by any family member, household member, enrolled child's family member and authorised nominee or visitor is strictly prohibited at any time.

The educator is responsible for setting clear and specific expectations regarding how family, household members, enrolled children's family members and authorised nominees and visitors should interact and behave with the children in their care, especially in relation to the use of devices. This includes:

- no exposure to inappropriate material via the TV, computer or phone
- no taking photos, recordings or videos of the children
- no taking photos, recordings and videos around, or **in the presence of the children.**
- no sharing of images or videos of FDC children that have been captured on a FDC Residence or venue CCTV device

Communication with families

Educators, must choose secure platforms that enable closed groups, and password protected access for sharing photos and communicating with families. It is the educators responsibility to ensure all families agree to not share images or videos on these sites that may include other children (*refer to Service register*)

Greater Hume Children Services staff

Staff and managers will adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the Educator's service.

The use of personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children in care is strictly prohibited. Staff and managers will report any concerns related to child safety, including inappropriate use of digital technology, to the approved provider or nominated supervisor.

Staff will only use Service issued electronic devices whilst visiting the Educators' Services. Staff will take images of children in care for the purpose of Educator Visit documentation. These images will be stored on visit sheets securely and deleted from Service issued devices as soon as visit sheet has been completed and stored securely.

Software programs and apps

Greater Hume Children Services staff and Educators use a range of secure software programs and apps to support the educational program and administration of the FDC Service. All apps used by staff, FDC educators, relief educators, visitors and children need to be carefully selected, regularly checked and kept up to date with the latest available system updates.

Access to software programs and apps need to be password protected to ensure the privacy of children, families, FDC educators and staff. Each user is required to create their own user account and ensure log in, and password information is not shared.

Any educational program software used by educators to share observations, photos, videos, daily reports, and learning portfolios with families will be in a secure, closed platform. The Approved provider will develop and maintain a register of all Apps and Platforms used.

Artificial Intelligence (AI) interactions and guidelines

Educators using AI are to be aware of limitations, privacy risks, and the potential for errors in the information it provides. Data and privacy concerns must be addressed, and educators should not enter details which may identify individual children, such as names and date of birth.

Confidential and Privacy guidelines

Greater Hume Council's *Privacy and Confidentiality Policy* applies to all use of digital technology and online environments. All staff, FDC educators, and visitors must ensure that any information, images, or digital content related to children, families, and the FDC Service is collected, stored, used, and shared in accordance with privacy legislation and FDC Service Policies, to maintain confidentiality and protect the safety and wellbeing of children.

Educators will inform the nominated supervisor as soon as possible regarding any potential threat to security information and access to data sensitive information, including lost or stolen devices.

Identification and reporting of online abuse and safety concerns

Greater Hume Children Services 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, FDC educators, relief 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 Safe Environment Procedure*)
- support FDC educators and relief 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 Protection Policy, Behaviour Guidance: Bullying 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.

Use of Closed-Circuit Television (CCTV) monitoring

Some educators may choose to use Close Circuit Television (CCTV) at the FDC Service residence or approved venue for the purpose of crime prevention strategies and Security and Surveillance.

Educators may use baby monitors to monitor children while they sleep. *[These do not replace any physical safe sleep checks]*. Access to the monitor is to be restricted through a password-protected system to ensure security and prevent unauthorised viewing.

Families are informed the FDC Service residence or approved venue uses CCTV as a surveillance method during enrolment and orientation to the FDC Service. Any recorded footage will be destroyed or de-identified when it is no longer needed for the purpose it was collected.

Breach of Policy

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

Links to Policy

Child Safe Policy
Code of Ethical Conduct Policy
Incident Injury Trauma and Illness Policy
Safe Rest and Relaxation Policy
Dealing with Complaints Policy
Dealing with Medical Conditions Policy
Fit and Proper Assessment of Family Day Care Educator Policy
Governance and Management of the Service Policy
Interactions with Children Policy
Monitoring and supervision of Family Day Care Educators
Privacy and Confidentiality Policy
Social Media and Internet Use Policy
Visitors to Family Day Care Residences and Venues Policy
Model Code of Conduct for Local Councils in NSW
Mobile Phone and Bring Your Own Device (BYOD) Policy

Links to Procedure

Child Safe Environment Procedure
Code of Conduct Procedure Including determining the Responsible Person
Dealing with Complaints Procedure
Dealing with Medical Conditions and Additional Needs Procedure

Incident Injury Trauma and illness Procedure
Interactions with Children Procedure
Monitoring and Support of educators Procedure
Privacy and Confidentiality Procedure
Social and Digital Media and Internet Procedure
Supervision Procedure

Links to Forms

Higher Risk Assessment Form
Visitor Sign in Sheet
Overnight and Out of Hours Care Form
Child Protection Work Process for Concerns
Digital Media Form
Incident Injury Trauma and Illness form
Medical Conditions and Additional Needs Risk Minimisation Plan
Medical Communication Plan

References

Nil

Responsibility

Director – Corporate and Community Services

Document Author

Manager Children Services

Relevant Legislation

NSW Child Protection (Working with Children) Act 2012
NSW Child Protection (Working with Children) Regulation 2013
NSW Children and Young Persons (Care and Protection) Act 1998
NSW Children's Guardian Act 2019
NSW Child Safe Standards
Victorian Child Safe Standards
NSW Children (Education and Care Services National Law Application) Act 2010
Privacy and Personal Information Protection Act 1998
Privacy Act 1998 (Cth.)
United Nations Convention on the Rights of the Child (1990)
National Quality Framework

Associated Records

Nil