Safe Use of Digital Technologies and Online Environments

Purpose Statement

Windermere Child and Family Services 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 National Model Code 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.

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, FDC educators, children, visitors and contractors, including online environments. We strive to create and maintain a positive digital safe culture that works in conjunction with our FDC 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, students, volunteers and visitors of the FDC Service.

Definitions

Refer to Appendix.

National Quality Standard (NQS)

QUALITY AREA 2: CHILDREN'S HEALTH AND SAFETY		
2.2.3.	Child Safety and Protection (effective Jan 2026) abuse or neglect.	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.
EDUCATION AND CARE SERVICES NATIONAL LAW AND NATIONAL REGULATIONS		
168(ha)	The safe use of digital technologies and online environments at the service	

Policy Statement

TO MAINTAIN CHILDREN'S SAFETY AND RIGHT TO PRIVACY, ALL DEVICES USED FOR FAMILY DAY CARE MUST FIRST BE APPROVED BY THE COORDINATION UNIT.

Safe Use of Digital Technologies and Online Environments

Procedures

Context

FDC 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. This usage must adhere to the following procedures.

Digital Technology and Electronic Devices Used in FDC

Our FDC Service adheres to the National Model Code for taking images or videos of children.

1. The approved provider will inform staff, FDC educators, educator assistants, visitors, volunteers and family members that the use of personal electronic devices used to take photos, record audio or capture videos of children who are being educated and cared for at the FDC 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) and other new and emerging technologies. These devices should not be in the possession of staff or visitors while working directly with children.
2. FDC educators may use and carry a personal electronic device while educating and caring for children and working directly with children, however these devices are NOT to be used to take or record images or videos of children.
3. The approved provider will inform staff 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 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)

Approved Service Devices for FDC Educators

How to request to register a business device/s for approval

1. To maintain compliance and safeguard children's privacy, **all** devices used for Family Day Care must first be approved by the Coordination Unit.
    - Educators will be required to submit details of their devices for approval via the below snap form

      FDC Application for Service Registered Device
    - Educators must have a business only email address at the time of application for a service registered device.
    - Only approved devices may be used to store, transfer, or manage Family Day Care records, including images of children and be accessed by the FDC Educator only.

- The Coordination Unit will assess the application within 3 business days, contacting the Educator to further discuss and complete a thorough risk assessment based on the Educator's unique setting.
- Should the requested device/s meet regulatory requirements the Educator will be provided an approval letter, approved device poster for display and completed risk assessment.
- The Educators families will receive an email of the Educators approved device/s and contact details to ensure their understanding and inclusion in the process.

Until a FDC business device/s is approved, Educators are not permitted to take images or videos of children while providing Early Childhood Education and Care.

2. Windermere FDC Service will maintain a register of all electronic devices purchased for and used within the FDC Service for both employees and Educators. This register will include details such as the identification/serial code, device type, intended use, assigned user, security settings, and any features related to connectivity, data storage, or recording capabilities.
3. Devices recorded in the register may include, but are not limited to, computers, tablets, mobile phones, cameras, CCTV systems, audio recorders, baby monitors, cameras, SD/memory cards, USB's and any other internet-connected or data-enabled devices used within the FDC Service.
4. Electronic devices approved by and registered with the FDC Service will be stored in a secure location at close of business and not utilised by any individual other than the FDC Educator.

Safe storage of digital content

1. Images and recordings of children must always be stored in a safe, secure, and private manner on an approved service device only.
2. Personal cloud services, social media, or unapproved applications **must not** be used for storing or sharing images. This means any device approved for taking/storing/sharing images must have iCloud or other cloud-based storage settings turned OFF.

   How to turn off iCloud Photos – Apple Support (AU)
3. All approved devices must be password protected, and access restricted to authorised users only (this should only be the Educator providing Education and Care).

Images and Videos

1. The approved provider is responsible for determining who is authorised to take, use, store and destroy images and videos of children using approved service issued digital devices.
2. Images and videos will be stored securely with password protection, with access limited to authorised personnel only.
3. 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.
4. FDC educators and FDC coordinators 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.
5. FDC Educators will only take images, recordings or videos of children with an approved service device whilst providing Education and Care as approved by the Windermere Coordination Unit.
6. FDC Educators will only store images, recordings or videos of children on approved service devices as approved by the Windermere Coordination Unit.

Safe Use of Digital Technologies and Online Environments

7. Our FDC Service will regularly review how digital data, including images and videos of children, is stored.
8. FDC Educators will not use cloud-based storage on any approved service devices. Digital data stored at the FDC Service will be destroyed in accordance with the *Record Keeping Policy*.
9. The approved provider and FDC educator will ensure staff, educators, visitors and volunteers do not transfer images or videos from FDC Service issued devices to personal devices. Unauthorised transferring of digital data may result in disciplinary action and/or Educator deregistration.

Physical Environment and Active Supervision

1. The approved provider, nominated supervisor, management and FDC educators will:
    a. Ensure children are always supervised and never left unattended whilst an electronic device is being utilised and/or connected to the internet
    b. 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 educators
    c. Reflect on our FDC Service residence or approved venue physical environment, layout and design to ensure it supports child safe practices when children are engaged in using technology
        i. Perform regular audits to identify risks to children's safety and changes in room environment set-ups that can indicate areas of higher-risk and become supervision 'blind spots'.
        ii. Only permit children to use devices in open areas where FDC educators can monitor children's use.
        iii. 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.
        iv. Ensure all visitors and volunteers are supervised at all times.
        v. Ensure all devices are password protected with access for FDC educators or staff only.
    d. Where digital devices are used during transportation and excursions, they must be used in accordance with practices outlined within this policy and associated procedure.
    e. Only utilise service approved devices for the purposes of taking, storing or sharing images or recordings of children.

Software Programs and Apps

1. Our FDC Service uses a range of secure software programs and apps on FDC Service-issued devices to support the educational program and administration of the FDC Service. All applications used by staff, FDC educators, visitors and children are carefully selected, regularly checked and kept up to date with the latest available system updates.
2. Access to software programs and apps are 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.
3. The approved provider will ensure programs which require additional background checks, such as CCS Software, are only accessed by authorised staff and FDC educators who have completed necessary screening processes in accordance with Family Assistance Law.

Safe Use of Digital Technologies and Online Environments

4. 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. In addition, our FDC Service may use accounting and payroll software. These platforms assist in managing the FDC Service's financial, staffing, and operational requirements.
5. Educator's may choose to utilise software or applications other than the services preferred platform Hubworks. Should an Educator choose to use another software platform or application for the purpose of programming, planning or sharing information they must first seek consent from families in writing via the 'consent to share information' form to utilise the chosen platform to share information, videos or recordings of their child. This consent to share information form must be completed for each child in care by a parent/guardian, a physical copy held on premise and a digital copy provided to the Coordination Unit.
6. An up-to-date log must be held on premise by the Educator in a secure location documenting parent/guardians' approvals/restrictions.

Artificial Intelligence (AI) Interactions and Guidelines

Important Alert: AI is embedded into many software applications. It is important to understand once information is entered into AI, there is a lack of data control of where it is stored, how it is managed and who has access to it. Information entered into AI is neither secure nor editable. AI can use facial and location recognition. There are currently no controls in place to manage the data in a secure way and limit public access.

1. Given the above risks, **Windermere does not permit staff or contractors to enter consumer data into any AI system** as it is likely to elevate risk of data leakage and privacy breach.
2. AI may be used to source online templates, forms and other information that **does not** involve personal, sensitive or other identifiable information about a FDC child, family member, staff member, educator or approved provider.

Confidentiality and Privacy Guidelines

1. Our 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 procedures, to maintain confidentiality and protect the safety and wellbeing of children.
2. Potential threats to security of information, unauthorised access to information (privacy breach) and loss of devices must be **reported at the time of the incident** by the educator to the Coordination Unit. Some examples of reportable incidents include:
    a. 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).
    b. A database with personal information about children and/or families is hacked.
    c. Personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report).
3. The nominated supervisor is to notify the approved provider **within 24 hours** of incidents related to point 2 above by emailing EducatorSupport@windermere.org.au and privacy@windermere.org.au

Safe Use of Digital Technologies and Online Environments

4. Where an incident is assessed as being a notifiable data breach as defined by the Office of the Australian Information Commissioner (OAIC), the Privacy & Information Sharing Officer and Manager FDC will submit an online report.

Identification and Reporting of Online Abuse and Safety Concerns

1. Our FDC Service will implement measures to keep children safe whilst using digital technology and accessing online environments.
2. The approved provider, nominated supervisor and management will:
    a. Ensure all staff, FDC educators, educator assistants, 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 (refer to Child Protection Policy).
    b. Support FDC educators and educator assistants to:
        i. Encourage children to seek support if they encounter anything unexpected that makes them feel uncomfortable, scared or upset.
        ii. 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.
        iii. Respond to and report any breaches and incidents of inappropriate use of digital devices and online services to management within **12 hours**.
    c. Ensure all concerns are documented and responded to promptly and appropriately, with support provided to the child and their family as required.
    d. Report any suspected cases of online abuse to the relevant authorities, including the e-Safety Commissioner and Police, in accordance with legal requirements and child protection procedures.
    e. 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.
3. The Royal Commission recommends that organisations engaged in child related work retain records relating to child sexual abuse that has, or is alleged to have occurred, for at least 45 years (Royal Commission into Institutional Responses to Child Sexual Abuse, 2017).

Use of Closed-Circuit Television (CCTV) Monitoring

1. Our FDC Service may have Educators using Closed-Circuit Television (CCTV) to monitor the physical environment of FDC Service residence and approved venues. Our FDC Service will regularly review guidance on the use of surveillance devices, including information provided by the Office of the Australian Information Commissioner.
2. Educators may choose to utilise baby monitors to monitor children while they sleep. Noting these **do not** replace any physical safe sleep checks or safe sleep practises.
3. Access to the monitor is restricted through a password-protected system to ensure security and prevent unauthorised viewing and is accessed on a service approved device. Families are informed

the FDC Service residence or approved venue uses CCTV as a surveillance method during enrolment and orientation to the FDC Service.

Camera Use

1. A sign will be placed at the entrance of the FDC Service to advise families and visitors about the surveillance. Closed-Circuit Television (CCTV) operates at the FDC Service and comprises of:
    - 3 fixed position cameras
    - A monitor
    - Digital Hard Drive Recorder
    - 1 Public Information Sign.

Camera Locations & Access

1. Camera locations **are** to include:
    - The entrance and exit points
    - Play room.
2. Cameras **are not** to be installed in private areas such as bathrooms or shower areas (for adults or children).
3. All cameras are to be clearly visible.
4. The CCTV recording system operates in real mode, monitoring the site continuously **24 hours a day**. Footage and information collected via the recording system will be governed by the *Australian Privacy Principles*. All relevant staff and FDC educators will be kept up to date with requirements under Australia's privacy law.
5. All recorded footage will be destroyed or de-identified when it is no longer needed for the purpose it was collected.
6. Access to CCTV footage at the FDC Service is strictly controlled and protected by secure, password-protected systems. Only authorised personnel are permitted to access the footage, in accordance with privacy laws and Service policies.
7. The approved provider is responsible for determining who is **authorised to access** CCTV footage. CCTV footage will not be accessible to staff members, other educators or families without appropriate authorisation.
8. The approved provider will enable access to CCTV footage for the purpose of investigations by Victoria Police, Child Protection and a Commissioner.

Responsibilities

Windermere Responsibilities

1. The approved provider, nominated supervisor, management and/or FDC Coordinator will ensure:
    - That obligations under the Education and Care Services National Law and National Regulations are met.
    - FDC educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and all related policies and procedures.

Safe Use of Digital Technologies and Online Environments

- All FDC Educators 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.
- 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.
- Have processes in place to ensure families who speak languages other than English understand the requirements of this policy, including providing authorisation for images and videos.
- Team members promote and support a child safe environment, ensuring adherence to the *Child Safe Environment and Child Protection Policies.*
- The National Principles for Child Safe Organisations is embedded into the organisational structure and operations
- All staff 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.
- Professional learning is provided to FDC educators and staff relating to the safe use of digital technologies and online environments
- The service will develop and monitor an Electronic Device Register for all electronic devices registered with and utilised by the FDC Service and used at the FDC Service/residence or approved venue
- All staff, FDC educators, family members, volunteers and students are aware of the National Model Code and Guidelines and **strictly** adhere to these guidelines for taking images or video of children including:
    - Personal electronic devices or personal storage devices are not used by FDC educators, educator assistants, family members, staff, visitors or volunteers to take images or videos when working directly with children.
    - Staff and FDC educators only use approved FDC Service registered electronic devices for taking, storing and sharing images or videos of children enrolled at the FDC Service.
    - FDC Service issued devices are securely configured, monitored and maintained to prevent unauthorised access.
- FDC educators and parents are aware of our FDC 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).
- The FDC Service Privacy and Confidentiality Policy is adhered to at all times by staff, FDC educators, families, visitors, volunteers and students.
- Images or videos of children must be appropriate in nature and must not show children in distress, in a position that may be perceived as sexualised or in a state of undress, including where genitalia may be exposed.
- External agencies or specialists are consulted if concerns are identified relating to online abuse, cyberbullying or digital safety risks.
- Collaborate with relevant professionals, as required, to support equitable access to digital technologies for all children.

Safe Use of Digital Technologies and Online Environments

- Educators 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 for all FDC educators.
- 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.

FDC Educator Responsibilities

FDC 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 Safe Environment and Child Protection Policies*, including mandatory reporting obligations.
- Adhere to Windermere's device application procedure, ensuring that only approved service devices are utilised to take, store and share images of children.
- Prominently display at the family day care residence the educators approved device poster.
- Ensure a physical copy of the educator's safe use of digital technologies and online environments risk assessment is available along with the approval letter for the safe use of digital technologies and online environments.
- Ensure that approved service devices are used and accessed by the Family Daycare Educator only.
- Ensure residents and visitors of the home are aware of their obligations and adhere to safe use of digital technologies and online environments in the home.
- 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 FDC Service's operations, including when accessing digital technologies and online learning environments.
- Not use personal electronic devices or non-approved service devices to take, store of share images or videos of children, access social media (Facebook, Instagram or other) or breach children and families' privacy while providing education and care at the FDC Service.
- Ensure written authorisation is obtained from parents/guardians to collect and share personal information, images or videos of their children online (Website, Facebook, Instagram or Educational Applications.

Safe Use of Digital Technologies and Online Environments

- Maintain a record of all children who are NOT to be photographed or captured on video is to be completed by the FDC Educator. This record will remain private and confidential.
- Keep passwords confidential and log out of computers and software programs after each use.
- Ensure consent forms are completed, provided to the coordination unit and stored on premise securely for all children in care.
- Create a physical and online environment that promotes safety and wellbeing while minimising the opportunity for children and young people to be harmed.
- Ensure parents/guardians are informed of how the FDC Service will take, use, store and destroy images and videos of children enrolled at the FDC Service during enrolment and orientation.
- 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 families are informed they may withdraw authorisation at any time by completing an updated consent form.
- Ensure children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online
- Ensure digital data is stored securely on an approved service device only, whether offline or online, and that data is archived regularly (monthly is recommended).
- Ensure images and videos are deleted or destroyed and removed from storage devices after being used for their intended purpose, uploaded to educational applications and included for documenting children's learning and development. Noting learning and development documentation must be held for **3 years** after the child's last day of attendance.
- Ensure images or videos of children must be appropriate in nature and must not show children in distress, in a position that may be perceived as sexualised or in a state of undress, including where genitalia may be exposed.
- 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.
- Cease use of the device immediately and report to the Coordination Unit should any changes occur regarding device utilisation.
- Report breaches of this policy to the Coordination Unit within **12 hours.**
- 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 per day.

Safe Use of Digital Technologies and Online Environments

- Ensure the use of TV/iPad and watching of DVD's is kept to a minimum, with programs chosen that are engaging and age appropriate to children. When used, the following conditions apply:
    - Only 'G' rated television programs and movies will be viewed at the FDC Service.
    - Programs depicting violence and/or inappropriate content (including graphic news reports) will not be shown.
    - TV programs or videos will only be shown that have positive messages about relationships, family and life.
    - Information about programs to be viewed will be shared with families beforehand to ensure.
    - That they approve of the content. Information may include title, synopsis, rating, length of program.
    - All content will be socially and culturally considerate and appropriate.
- Strive to share information to families about recommended screen time limits based on Australia's Physical Activity and Sedentary Behaviour Guidelines.
- Ensure all documentation and records relating to safe use of digital technologies are kept safe and secure for a period of **3 years** following the child's last day of attendance.

Family Responsibilities

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 FDC Service.
- Provide written authorisation indicating whether or not the FDC Service and FDC educator may take, use, store or destroy images or videos of their child.
- Provide written notification if they wish to withdraw the authorisation for the Service to take, use, store or destroy images and videos of their child.
- Be requested to provide written authorisation/consent for individuals visiting the Service to take photographs of their child/ren (e.g. ECIP professionals, professional photography for marketing, school photos etc.).
- Be able to withdraw authorisation for the Service to take, use, store or destroy images or videos of children at any time in writing.
- Be aware that sometimes other children in the FDC 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.

Safe Use of Digital Technologies and Online Environments

Visitors, Volunteers and Family Members' Responsibilities

These groups will:

- Adhere to the *Safe Use of Digital Technologies and Online Environments Policy* and associated procedure whilst visiting the FDC 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 FDC 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 and the approved provider to capture images or video of a child for observation/documentation purposes only. This applies to visitors who are supporting children at the FDC Service (NDIS funded support professionals, Inclusion Support professionals) (See ECIP Confidentiality Agreement).

Breach of Policy

1. Staff members or FDC educators who fail to adhere to this policy may be in breach of their terms of engagement and may face disciplinary action which may lead to notification to the regulatory authority and child protection authorities and termination of their engagement.
2. 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 FDC Service.

Standards

- National Quality Framework for Early Childhood Education and Care Services including Education and Care Services National Law & Regulations 2011
- Victorian Child Safe Standards
- Rainbow Tick Standards.

Relevant Legislation

- Child Care Subsidy Secretary's Rules 2017
- A New Tax System (Family Assistance) Act 1999
- The National Model Code 2024
- Family Law Act 1975
- Privacy Act 1988
- Family Assistance Law – Incorporating all related legislation as identified within the Child Care Provider Handbook

Related Policies & Links

- Safe Use of Digital Technologies and Online Environments Policy
- 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

Safe Use of Digital Technologies and Online Environments

- 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)

Continuous Improvement/Reflection

Our *Safe Use of Digital Technologies and Online Environments Policy* will be evaluated and reviewed on an annual basis or earlier if there are changes to legislation, ACECQA guidance or any incident related to our policy. Feedback will be requested from children, families, staff, educators and management and notification of any change to policies will be made to families within 14 days.

For queries or concerns related to this policy, contact the FDC Coordination Unit:
enquiriesECECS@windermere.org.au

Safe Use of Digital Technologies and Online Environments

DEFINITIONS	
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.
Harmful content	Harmful content includes sexually explicit material; false or misleading information; violence; extremism or terrorism; hateful or offensive material
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