

Safe Use of Digital Technology and Online Environments Policy

1. Purpose

In accordance with the Education and Care Services National Regulations, an Approved Provider must ensure that policies and procedures are implemented for the safe use of digital technologies and online environments within the service.

My Place Family Day Care (FDC) is committed to maintaining a child safe environment that upholds the principles of the National Model Code for Taking Images or Videos of Children while Providing Early Childhood Education and Care and meets the requirements of the Queensland Child Safe Standards.

This policy applies to all aspects of the service's digital presence and practices. It provides clear guidance for the service and its Educators in relation to:

- The taking, use, storage and destruction of images and videos of children attending the Service.
- Obtaining authorisation from parents to take, use and store images and videos of children attending the service.
- The use of any optical surveillance devices at the service (e.g. CCTV).
- The use of digital devices by children attending the service.

2. Scope

This policy applies to the Approved Provider, My Place FDC Manager and all other Nominated Supervisors, Coordinators, Educators, Educator Assistants, parents and children in care.

3. Definitions

Approved Provider: Inala Community House (ICH) has approval from the Federal Government to operate an approved FDC service.

Service: My Place Family Day Care, whose Approved Provider is Inala Community House.

Parent/Guardian: The person responsible for the payment of fees and who is paid the Child Care Subsidy. Referred to as the Parent/s. PLEASE NOTE: this does not include a parent who is prohibited from having contact with the child by an order of a court, tribunal or department responsible for Child Safety.

Educator: A suitably qualified person who is registered with the service.

Internet: Refers to the world wide web of computer systems that facilitates the transmission and exchange of data. Information search engines and web browsers include, but are not limited to, Google, Firefox and Internet Explorer.

Social Networking Media: Refers to any online tools or functions that allow people to communicate or share information via the internet. This includes, but is not limited to, applications such as Facebook, YouTube and Twitter.

Mobile device: Refers to devices that have non-Wi-Fi internet access such as iPads, tablets, iPods, and mobile phones.

ICT: Information and Communication Technology.

Closed Circuit Television (CCTV): Is visual surveillance technology that uses video cameras to transmit a signal to a specific, limited set of monitors. The term "closed circuit" signifies that the footage is not publicly broadcast but is instead monitored privately.

Cyber Safety: Safe and responsible use of the internet and equipment/devices, including mobile phones and devices.

Cyber-bullying: Involves the deliberate, repeated, and hostile use of information and communication technologies by an individual or group that is intended to harm, intimidate, or distress others.

E-crime: Occurs when a computer or other electronic communication device (e.g. mobile phone) is used to commit an offence, is targeted in an offence, or acts as a storage device for evidence of an offence.

Informed Consent: A legally sound and clear process where families are given all necessary information about how and why their child's images or videos will be taken, used, and stored. This includes details on the specific purposes, a clear understanding of potential risks, and the explicit right to withdraw consent at any time. The consent must be freely given and documented in writing, and the service must also respect a child's right to refuse consent even if a parent has provided it.

4. Policy

My Place FDC is committed to a child-centred approach in all matters relating to digital technology and online environments, placing the safety, wellbeing, and best interests of every child at the core of our practice. We acknowledge the important role that digital platforms can play in children's learning, communication, and play, while recognising the potential risks they present.

My Place FDC also acknowledges that Educators may install Closed Circuit Television (CCTV) systems or other security and monitoring devices such as doorbell cameras, in various internal and external locations throughout their approved family day care property. These systems can contribute to the overall safety and security of children, Educators and premises. However, My Place Family Day Care is committed to balancing these security benefits with the paramount rights to privacy and dignity of all individuals, particularly children.

The priority of My Place FDC is to provide a safe, respectful, and inclusive digital environment that protects children from harm, upholds their rights, and supports their healthy development. My Place FDC will take all reasonable steps to protect children from all forms of harm, exploitation, abuse, and discrimination, which includes preventing exposure to inappropriate content, protecting their personal data and privacy, and safeguarding their digital reputation.

The taking, storing, and sharing of images and videos, will only be done with explicit consent from parents or guardians. These images will be used for legitimate, child-centred purposes, always respecting the dignity, privacy, and cultural identity of children and their families. The

primary purpose of CCTV and other security/monitoring footage is to enhance safety and security and where it is used within a family day care residence, clear signage will be visible at the entrance to the residence and written acknowledgement will be provided by families. CCTV and other security/monitoring footage will not be used for any purpose other than routine surveillance of the premises.

My Place FDC will continuously review and adapt our procedures to ensure staff and Educators are provided with current and up-to-date information on the secure storage and disposal of data which includes images and videos of children, ensuring compliance with privacy laws and regulations.

5. Responsibilities

Approved Provider:

- Ensure all obligations under the Education and Care Services National Law and National Regulations are met, with a specific focus on digital safety and child protection in online environments.
- Ensure the National Principles for Child Safe Organisations and Queensland Child Safe Standards are embedded into the organisational structure and operations.
- Ensure Educators, Educator Assistants, staff, visitors and volunteers are made aware of the Safe Use of Digital Technologies and Online Environments for Children Policy and the associated procedures are fully implemented to safeguard children's health, safety, and wellbeing.
- Take all reasonable and necessary steps to ensure the Coordination Team, Educators, Educator Assistants, other staff and volunteers consistently follow the Safe Use of Digital Technologies and Online Environments for Children Policy and associated procedures, with regular monitoring and accountability procedures in place.
- Actively promote and embed a culture of child safety and wellbeing that underpins all aspects of the service's operations, including online learning environments and digital interactions, specifically to reduce all forms of risk to children (including the risk of abuse, exploitation, and inappropriate exposure).
- Ensure all digital devices issued to Coordination Team or other staff are securely configured, monitored and maintained to prevent unauthorised access.
- Ensure all images and videos of children taken by the Coordination Team during the course of their work are backed up as required, stored securely and disposed of in accordance with relevant procedures.
- Ensure all Educators with closed circuit (CCTV) systems or other security monitoring devices (e.g. doorbell cameras) installed in their residence are aware of their legal responsibilities for the safe use, secure storage and permanent disposal of all CCTV recordings.
- Ensure current copies of the policy and procedures are readily accessible to all stakeholders (children, families, staff, volunteers) and are available for inspection, promoting transparency in our safety practices.

Coordination Team (Nominated Supervisor, Coordinator/s):

- Rigorously implement the Safe Use of Digital Technologies and Online Environments for Children Policy and Procedures and ensure risk management plans are in place for all digital activities, where relevant.

- Ensure all staff, Educators, Educator Assistants and volunteers are provided with a copy of this policy and procedure as part of a comprehensive induction process and advised of where this policy can be accessed.
- Provide ongoing and comprehensive training to all Educators, Educator Assistants and volunteers to ensure they understand how to actively and vigilantly supervise children where they may be using digital technologies within their program, including monitoring screen content and interactions.
- Maintain ongoing, transparent communication with Educators, Educator Assistants and staff about their responsibilities and any changes to policies, procedures, and relevant legislation, particularly as digital technologies and online risks evolve rapidly.
- Actively support Educators, Educators Assistants and Coordination Team staff to uphold the service's robust culture of child safety and wellbeing across all operations, including when accessing digital technologies and online learning environments.
- Ensure all Educators, Educator Assistants, volunteers and other staff are aware of current child protection laws, child safe practices and their duty of care to ensure that reasonable steps are taken to prevent harm to children.
- Support Educators and Educator Assistants to fully understand the National Model Code and effectively manage their use of electronic and digital devices within their program, as appropriate to service context.
- As required, regularly back up all images and videos of children taken by the Coordination Team during the course of their work and ensure they are stored securely and disposed of in accordance with the procedures of this policy.
- During enrolment and orientation, ensure parents/guardians are informed of how the Service will take, use, store and dispose of images and videos of children enrolled at the Service.
- Request that parents/guardians provide explicit written consent for images and videos of their child to be taken, used and stored during their child's enrolment with the Service, including social media (Facebook, Instagram) and the Service's digital documentation software.
- Advise parents/guardians that their consent for images and videos of their child can be revoked in writing at any time.
- Where consent for images and videos has been revoked in writing by a parent/guardian, ensure all images and videos of their child are deleted or destroyed and removed from storage.
- Ensure written authority is obtained from parents/guardians for children to use digital devices and technology at the family day care residence.
- Ensure images and videos of children in care 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.
- Ensure Educators with closed circuit (CCTV) or other security monitoring devices (e.g. doorbell cameras) have clear signage indicating the presence of CCTV and/or other security monitoring devices displayed prominently at the entry to their approved family day care residence.
- Where relevant, ensure families are made aware and have provided written acknowledgement of the presence of CCTV and/or other security monitoring devices installed within the approved family day care residence.
- Ensure Educators adhere to all regulatory and privacy requirements for the secure storage and access of all images and videos of children including any CCTV/security monitoring footage (where relevant).
- Ensure families are made aware of this policy and associated procedures and how to access them.

Educators/Educator Assistants:

- Implement the Safe use of Digital Technologies and Online Environments for Children Policy and Procedures to ensure children's safety and wellbeing.
- Consistently uphold the service's culture of child safety and wellbeing in all interactions, with particular vigilance when accessing digital technologies and online learning environments.
- Actively participate in ongoing and comprehensive training related to digital safety, privacy protection and responsible use of digital technology within their program.
- Ensure active constant, and vigilant supervision of children when using digital technologies as part of their program, including by monitoring screen content and interactions to keep children safe.
- Recognise and respond effectively to children and young people when discussing the use of digital technologies and online environments, considering their diverse needs, interests, and developmental stages, and empowering them to report concerns.
- Ensure they fully understand the National Model Code as appropriate to service context, and the service's explicit expectations around the taking, sharing and storage of children's images or videos while at the service and proactively seek guidance when needed from the Coordination Team regarding any digital safety concerns or uncertainties, including respecting a child's right to refuse to have their image taken or shared, even if prior parental consent has been provided.
- Ensure written consent has been provided by a child's parent/guardian for images and videos of their child to be taken, used and stored during their child's time in care. Be aware, this consent can be revoked in writing at any time.
- Ensure images or videos of children are not taken, used or stored without prior consent from a child's parent/guardian.
- Ask children's permission before taking photos of them on any device and explain to children how photos of them will be used and where they may be published, to ensure their voices are heard and respected in a meaningful way.
- Introduce concepts and 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.
- Not use images or videos of children on social media platforms (Facebook, Instagram) or digital documentation programs without the express written consent of parents/guardians, including consent for where they may be shared. This includes ensuring children's personal information where children can be identified such as name, address, age, date of birth etc. is not shared online.
- Where consent for images and videos has been revoked in writing by a parent/guardian, ensure all images and videos of their child are deleted or destroyed and removed from storage.
- Ensure images and videos of children in care 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.
- Ensure visitors and family members do not use any personal electronic devices, including mobile phones, smart watches or META sunglasses to take images and videos or record audio of children at the Service.
- Where relevant, ensure clear signage is displayed prominently at the entry to their approved family day care residence, indicating the presence of CCTV and/or other security monitoring devices.
- Where relevant, ensure families are made aware and provide written acknowledgement of the presence of CCTV and/or other security monitoring devices installed within the approved family day care residence.

- Adhere to all regulatory requirements for the secure storage, access and disposal of all images and videos of children including any CCTV/security monitoring footage (where relevant).

Visitors, volunteers and family members residing at the FDC residence:

- Adhere to the Safe Use of Digital Technologies and Online Environments for children Policy and associated procedure whilst visiting the FDC residence at times when children are in care.
- Not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children in care at the FDC Residence.
- Report any concerns related to child safety, including inappropriate use of digital technology, to the Approved Provider or Nominated Supervisor.
- Ensure written consent is provided by parents/guardians to capture images or video of a child for observation/documentation purposes only. This applies to allied health professionals (Inclusion support professionals, NDIS funded support professionals, etc.) who may be supporting children at the Educators' FDC residence.

Families:

- Read, understand and adhere to the Service's policies and procedures regarding the Safe use of Digital Technologies and Online Environments for Children.
- Not duplicate or upload to the internet or any social media platform (e.g. Facebook, Instagram) any photos of their own child that may at times also capture the image of other children.
- Actively support and reinforce the Service's expectations regarding the use of children's personal digital devices while at the Service, understanding these are in place for the safety of all children.
- Provide explicit written consent for images and videos of their child to be taken, used and stored by the Service and Educator for the purposes of documenting their experiences and learning during their time in care.
- Not use personal electronic devices, such as mobile phones, smart watches or META sunglasses, to take photos, record audio, or capture video of children at the Educators FDC residence.
- Promptly raise any concerns about the safe use of personal devices and/or the internet with the Nominated Supervisor, working in collaboration to address potential risks.

6. Review

This policy shall be reviewed at a minimum every two years.

This policy remains in effect unless otherwise determined by resolution of the Board of Directors.

	Date	Details
V1.0	1/09/2025	Original policy issued

7. Related Documents

Policies

1.4 Code of Conduct
2.1 Interactions with Children Policy
2.2 Child Protection Policy
2.5 Acceptance and Refusals of Authorisation Policy
3.1 Educational Program and Practice Policy
6.1 Child Safe Environment Policy
9.1 Enrolment and Orientation Policy
ICH FDC Managing FDC Register and Notifications Policy

Procedures

2.1 Interactions with Children Procedure
2.5 Supervision of Children Procedure
2.11 Acceptance and Refusals Procedure
3.1 Education Program and Practice Procedure
6.6 Providing a Child Safe Environment Procedure
9.2 Enrolment and Orientation
10.5 Confidentiality and Privacy Procedure
10.6 Record Management and Storage Procedure
ICH FDC Managing FDC Register and Notifications Procedure

Forms

Parent consent form for taking, sharing and storage of images and videos
CCTV Acknowledgement form

References

Education and Care Services National Law 2010:

- S. 162A Child Protection Training
- S. 165 Offence to inadequately supervise children
- S. 167 Offence relating to protection of children from harm and hazard

Education and Care Services National Regulations:

- R. 73 Education Program
- R. 76 Information about educational program to be given to parents
- R. 84 Awareness of child protection law
- R. 115 Premises designed to facilitate supervision
- R. 155 Interactions with children
- R. 156 Relationships in groups
- R. 165 Record of visitors
- R. 166 Children not to be alone with visitors
- R. 168 Education and Care Services must have policies and procedures
- R. 169 Additional policies and procedures – family day care service
- R. 170 Policies and procedures to be followed
- R. 171 Policies and procedures to be kept available
- R. 172 Notification of change to policies or procedures
- R. 175 Notification of change to policies and procedures
- R. 176 Time to notify certain information to Regulatory Authority

- R. 176A Prescribed information to be notified to approved provider by family day care Educator
- R. 179 Family Day Care Educator to provide documents on leaving service
- R. 181 Confidentiality of records kept by approved provider
- R. 182 Confidentiality of records kept by family day care Educator
- R. 183 Storage of records and other documents
- R. 184 Storage of records after service approval transferred

ACECQA, Guide to the National Quality Framework, 2018, Chapter 2 The National Quality Standards:

- Quality Area 1 - Educational Program and Practice
- Quality Area 2 - Children's Health and Safety
- Quality Area 5 - Relationship with Children
- Quality Area 6 - Collaborative Partnerships with Families and Communities
- Quality Area 7 - Leadership and Management

Additional Regulatory Context and Guidance:

- Working with Children (Risk Management and Screening) Act 2000 (Qld)
- Criminal Code Act 1899 (Qld)
- Online Safety Act 2021 (Cth)
- eSafety Commissioner - Best Practice Framework for Online Safety Education
- eSafety Commissioner - [eSafety Early Years program for educators](#)
- ACECQA [PolicyGuidelines SafeUseOfDigitalTechOnline final.pdf](#)
- [NQF Online Safety Guide 1.pdf](#)
- [NQF Child Safe Culture Guide | ACECQA](#)
- [Child Safe Standards | Queensland Family and Child Commission](#)
- [National Model Code Taking Images and Videos.pdf](#)
- Privacy Act 1988