# Safe Use of Digital Technology and Online Environments Procedure

## 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 procedure 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 procedure applies to the Approved Provider, Nominated Supervisors, Coordinators, Staff, 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 by a court order from having contact with the child
Educator: A suitably qualified person who is registered with the service.

**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. Procedure

### *4.1* Penalties for breaching regulatory requirements

Under the Education and Care Services National Law and Regulations, penalties may apply to Approved Providers and FDC Educators in relation to:

- Offence relating to inadequate supervision of children (s.165 of the Law)
- Offence relating to protection of children from harm and hazards (s.167 of the Law)
- Nominated Supervisor, any staff members, volunteers and students at the service who work with children are advised of the existence and application of the current child protection law and any obligations they have under this law (regulation 864).
- Children's enrolment record to be kept (Regulation 160)
- Record of all visitors to FDC residence while education and care is being provided (Regulation 165)
- Policies and procedures to be followed (Regulation 170)
- Policies and procedures to be kept available (Regulation 171)
- Prescribed enrolment and other documents to be kept by family day care educator (Regulation 178)
- Confidentiality of records kept by approved provider (Regulation 181)
- Confidentiality of records kept by family day care educator (Regulation 182)

**Penalties for breaching these regulatory requirements may be as high as $57,400.**

## *4.2* Digital Technology and Electronic Devices Used at the Service

Visitors, volunteers and family members will be informed 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 the use of items such as tablets, iPads, mobile 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).

Explicit written consent will be required from parents/guardians before any visitor or volunteer captures images or videos of a child. This includes, but is not limited to, incursion providers, practicum students, Inclusion Support professionals, or NDIS funded support professionals. This consent is necessary for any image or video captured for professional observation or documentation purposes.

### *4.2.1 Service Issued Device Use*

My Place FDC will provide digital devices to members of the Coordination Team or other approved staff members for work related purposes, including the monitoring of Educator practices. This may involve taking images, videos or recording audio of children as part of their professional duties.

Members of the Coordination Team may carry their own personal devices during home visits to ensure their own and others safety, if needed. Personal devices will not under any circumstances be used to take photos without approval of the FDC Manager. If this is done in exceptional circumstances, the photos will be immediately downloaded and permanently deleted from the staff members device upon arriving back to the Service office.

### *4.2.2 Educator Owned Device Use*

My Place FDC acknowledges that Educators may use their own personal digital device to conduct their work, however, to safeguard children's safety and privacy, My Place FDC recommends Educators use a separate FDC only device for taking images, videos or recording audio of children to document their learning and participation in the program. Educators will receive comprehensive guidance on the ethical use of digital devices in line with the National Model Code. This includes strict protocols for taking photos or videos of children for Educator-led experiences as well as their storage, use and secure disposal. Explicit written consent from parents/guardians will be required for all children involved to ensure their privacy and dignity are respected.

Educators and Educator Assistants will be provided with comprehensive guidance and instruction on the safe use of digital technologies and keeping children safe from harm. Any intentional misuse of an Educator owned device for a purpose such as online bullying, harassment or image-based abuse will be thoroughly and immediately investigated and reported to the Regulatory Authority and other relevant child protection authorities as required.

### *4.2.3 Children's Access to Digital Technology and Devices*

In line with My Place FDC's commitment to children's health and wellbeing, Educators will purposefully limit access to digital technology and devices (screen-time) within their program. Any leisure screen time will be restricted, with clear times set out in their program and strict supervision protocols in place. When children have access to technology and/or

devices owned by the Educator, the content must be age-appropriate for the children, using government classifications (G rated) and under the direct supervision of the Educator. Permission from the child's parent/guardian will be obtained for children to access any digital technologies.

Children may only access personal devices with the express written permission of their parent/guardian and only if appropriate filtering and monitoring systems are confirmed to be in place on the device. Children using personal devices, whether connected to the internet or not, must be actively supervised by the Educator, who must be able to view their screens at all times to ensure appropriate content. Children must not be left unattended whilst using any electronic device and children's personal devices are not permitted to connect through the Educator's internet provider.

To protect privacy and prevent misuse, children will not be permitted to take photos, videos or recordings of other children on their own personal devices under any circumstances. Should a child be found to be accessing inappropriate content or using the camera on their device, immediate action will be taken, the parent/guardian will be advised of the incident and future restrictions will be imposed to ensure the safety of all children.

## *4.3* Taking of images and videos

Images and videos of children must be taken and used in strict accordance with the National Model Code. They will only be captured for educational or documented learning purposes, never for gratuitous or personal reasons.

During monitoring visits, the Coordination Team will discuss with Educators the intent, appropriateness, context and consent involved in capturing and using images and videos. This process ensures that the use of these images aligns with children's learning, wellbeing and their right to privacy.

The service will ensure that all parental consent is informed, written, and revocable. There will be a clear distinction between internal use (e.g., in a child's learning journal) and external use (e.g., on a public-facing social media page). All parental consent information will be provided to the Educator before the child begins care.

Educators will actively teach children about their right to privacy and empower them to say "no" to being photographed or filmed. This decision will be immediately respected, regardless of whether a parent has given consent, as the child's right to privacy takes precedence.

## *4.4* Safe Storage of Images and Videos of Children

### *4.4.1 Service Storage*

My Place FDC will ensure all digital images and videos taken by the Coordination Team on service issued devices are stored on encrypted, service-owned storage devices or cloud services. Access will be managed through multi-factor authentication and limited to authorised personnel. The storage of these images on personal devices, including staff phones or personal cloud accounts, is strictly prohibited.

The Service will regularly review its digital storage systems to ensure compliance with this policy. This includes verifying that images are stored correctly, that access is authorised and

that all data related to exited children has been properly and permanently deleted, where relevant.

**Data Transfer and Secure disposal**

To prevent data loss and unauthorised access, all images and videos captured by the Coordination Team will be securely transferred and uploaded to the service's web-based platform (Harmony) as needed on a regular basis. Once transferred, the images will be immediately and permanently deleted from the device's local storage.

When a child leaves the service, all digital images and videos related to that child will be permanently deleted from all storage locations within a defined timeframe (e.g., 30 days post-enrolment end) or in accordance with prescribed documentation retention periods. A formal log will be maintained to record the date and method of disposal. For printed materials, secure shredding or incineration will be used.

### *4.4.2 Educator Storage*

My Place FDC recommends Educators do not store images and videos of children on cloud-based storage systems in the Educators home or other private locations, on portable devices such as SD card or USB devices (long term), or on a device that may be used by other members of the family.

It is recommended that Educators use a secure device specifically for family day care use, if available. Families will be advised during enrolment to speak with the Educator to confirm their process for the storage of images and videos.

## *4.5* Software Programs, Apps and Artificial Intelligence (AI)

My Place FDC uses an online documentation software program (Harmony) that enables Educators to share observations, photos, videos, daily reports, and learning portfolios with families through a secure, closed platform. Access is password protected to ensure the privacy of children, families, and Educators. Each parent account holder is required to create their own user account and ensure log in, and password information is not shared.

The Approved Provider will ensure programs requiring additional background checks, such as CCS Software, are only accessed by authorised staff and Educators who have completed necessary screening processes in accordance with Family Assistance Law.

Educators using educational software programs or Apps as part of their program must ensure they are age-appropriate and that devices used have appropriate and regularly updated filtering and monitoring systems and controls in place.

When using AI, Educators and Coordinators must be aware of its limitations, privacy risks, and the potential for errors. AI can be a useful tool but is the responsibility of the user to ensure the accuracy of the information it provides. No details that could identify individual children, such as names and date of birth should ever be used with AI.

## *4.6* Confidentiality and Privacy

The Privacy and Confidentiality Policy applies to all use of digital technology and online environments. All Nominated Supervisors, Coordinators, 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 immediately advise the Approved Provider of any potential threats to data security. My Place FDC will follow all relevant policies, procedures and practices to protect sensitive digital data.

If there is any suspicion that an e-crime has been committed, a report will be made to the police. If there is a reasonable suspicion that evidence of a crime is contained on a service issued or Educator's device it will be made available to the investigating police officer wherever possible and without delay. The electronic device should not be tampered with. The Service may also be required to complete an Incident, Injury, Trauma and Illness report and notify the Regulatory Authority as per the Managing FDC Register and Notifications Policy, ensuring all legal and ethical reporting requirements for child safety are met.

The Approved Provider will notify the Office of the Australian Information Commissioner (OAIC) in the event of a possible data breach. This could include:

- A device containing personal information about children and/or families is lost or stolen (parent names and phone numbers, dates of birth, allergies, parent phone numbers)
- A data base with personal information about children and/or families is hacked
- Personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)
- Any possible breach within the Service or if the device is left behind whilst on an excursion

## *4.7* Use of CCTV Data

Through comprehensive induction and ongoing training, Educators and Educator Assistants will be made aware of their mandatory reporting requirements to report any concerns related to child safety including inappropriate use of digital technology to the Approved Provider or Coordination Team.

Educators and Educator Assistants will actively encourage children's safe and responsible use of digital technology and devices through a range of proactive strategies including, but not limited to:

- Monitoring what children are looking at/for when accessing the internet, ensuring content is age-appropriate and safe
- Engaging in regular, age-appropriate conversations with children about their concept of 'the internet' and 'being online,' intentionally teaching them about safe online behaviours, privacy, and how to report anything that makes them feel uncomfortable or unsafe
- Empowering children to understand and exercise their right to have an image or video of them removed or not taken at all

## 5. Review

This procedure shall be reviewed at a minimum every two years in conjunction with relevant policies.

| | Date | Details |
|---|---|---|
| V1.0 | 5/09/2015 | Original procedure issued |

## 6. Related Documents

**Policies**

ICH FDC Safe use of Digital Technology and Online Environments Policy