Building Futures Care Digital Technology Policy and Procedure

PURPOSE

This policy outlines Building Futures Care's commitment to managing digital technologies in accordance with proposed Regulation 2.11 relating to the use, management and oversight of digital technologies in family day care, ensuring digital practices support child safety, privacy, supervision, risk management and regulatory compliance.. It ensures the protection of sensitive and confidential information and promotes the appropriate, ethical and secure use of digital devices, photographs, videos and data management systems. This policy is developed in line with the National Model Code for taking Images of Children in Early Childhood Education and Care and its associated guidelines, reinforcing child safe practices when capturing, storing and sharing images. It supports a culture of transparency, accountability and respect for children's rights, privacy and dignity in all digital practices.

POLICY STATEMENT

Building Futures Care recognises that digital technologies present both opportunities and risks. Their use in family day care must always prioritise child safety, active supervision, privacy, professional boundaries and ethical practice. Digital technologies must support, and never compromise, the wellbeing, dignity and rights of children.

Building Futures Care recognises that digital technologies are essential for communication, documentation and record keeping. We are committed to safeguarding all personal, sensitive and confidential information through the secure, ethical and responsible use of digital tools. All educators, staff, visitors, students and volunteers are required to adhere to this policy to protect privacy and comply with legal obligations under the Privacy Act 1988, the Notifiable Data Breaches Scheme, and the requirements of the National Quality Framework (NQF), including the Education and Care Services National Law and National Regulations.

Building Futures Care permits educators in family day care settings to have personal digital devices on their person while working directly with children; however, their presence must never interfere with active supervision or educator responsiveness to children. The use of personal mobile phones, tablets, smartwatches or any unauthorised devices to photograph, film, record, store or share images or information relating to children is strictly prohibited and not permitted by the service. Protecting children's privacy, maintaining confidentiality, and upholding professional boundaries are priorities at all times.

RESPONSIBILITIES

Approved Provider and Nominated Supervisors must:

- Monitor compliance with Regulation 2.11
- Understand their legal and ethical obligations related to digital technology use.
- Formally authorise devices for capturing, storing and transmitting images.
- Maintain a **Service Device Register** of all service-supplied and service-authorised devices recording Device name, Device model and serial number, user/educator assigned, whether service supplied or service authorised, date authorised, device deauthorisation/removal date.

- The Service Device Register will also record any **associated work laptops/computers and approved software platforms** used by educators for storing and managing children's documentation to support oversight, security and audit compliance.
- Ensure authorised devices used within the service are implemented with appropriate security measures, including password protection, secure storage of information, and the use of approved platforms to protect children's privacy and prevent unauthorised access to images, records, or communications.
- Take reasonable steps to prevent personal device misuse.
-

Educators, Coordinators, Students and Volunteers must:

- Maintain active supervision while using authorised technology
- Use ONLY service-supplied or service-authorised devices for images of children.
- Never use personal devices to photograph, film, record or share children's images.
- Request families not to copy, download, screenshot or share photographs or videos from educator documentation, social media pages or communication platforms
- Protect passwords and access credentials
- Not use service devices for personal purposes.
- Immediately report suspected breaches.

PROCEDURES

DIGITAL INFORMATION SECURITY & DEVICE MANAGEMENT

All service-supplied and service-authorised devices must:

- Devices used for service purposes must be secured with a password, PIN or biometric lock, with automatic screen lock enabled.
- Where available, multi-factor authentication and updated security software should be used to help keep information safe.
- Devices should be stored securely when not in use, not left unattended in vehicles or public places, and service information should only be accessed through secure networks and approved service accounts.

DIGITAL TECHNOLOGIES AND ACTIVE SUPERVISION

Educators must ensure use of digital technology does not compromise active supervision, engagement or responsiveness to children.

Requirements:

- Digital devices must not distract educators from supervision responsibilities.
- Documentation, messaging and digital administration should occur when it does not interfere with direct child supervision.
- Devices must not be used for personal browsing, calls, messaging or social media while educating and caring for children, except in emergencies.

- Use of digital technologies must always support, not replace, educator-child interactions.

PERMITTED USE:

- Only service-supplied or service-authorised devices (including approved digital cameras, tablets/iPads, mobile phones and other authorised recording devices recorded on the Service Device Register) may be used to capture images of children.
- Images must only be uploaded to approved service platforms or work-designated systems using secure, password-protected devices, including service-approved laptops or desktop computers.
- Devices must be used solely for professional purposes and in accordance with service privacy, consent and documentation requirements.
- Images must be transferred promptly to approved systems and deleted from the original device once securely uploaded.
- Images must not be stored on personal devices, personal cloud accounts, USBs or unauthorised applications.
- Devices must be used in a way that maintains active supervision and protects children's privacy, dignity and confidentiality at all times.

SURVEILLANCE

Where CCTV is installed:

- Families must be informed at enrolment.
- Clear signage must be displayed.
- Access must be restricted to authorised persons.
- Footage must be securely stored and destroyed appropriately.

STORAGE AND ACCESS TO DIGITAL INFORMATION

- Digital information must not be downloaded to personal devices.
- Families have the right to access their own child's records upon request.
- Educators may share information with Coordinators or other educators only when necessary to support the wellbeing and care of the child.
- Families will be notified if their data has been lawfully shared with an external agency.

SOCIAL MEDIA AND ONLINE CONDUCT

Educators and staff must:

- Never post children's images on personal social media.
- All public sharing of children's content must be in accordance with signed permissions and scheme guidelines
- Personal opinions, grievances, or confidential matters must not be discussed online.

- Closed family groups (such as those on What's App, Facebook, etc) used to share images and children's experiences must be limited to currently enrolled families. Access to these groups will end when a family is no longer actively enrolled, to ensure privacy and maintain appropriate communication within the current care community.

SERVICE / HOME-PROVIDED DIGITAL DEVICES ACCESSED BY CHILDREN IN CARE

- Written parental authorisation required.
- Parental controls must include:
  - Age-appropriate app restrictions
  - Safe browsing filters
  - Time limits
  - No camera access
- Devices used only under supervision.
- Screen time must align with current health guidelines.
- Devices must not replace active engagement.

NOTIFIABLE DATA BREACHES SCHEME

In the event of a suspected or actual data breach:

- Immediately report to the Nominated Supervisor or Building Futures Care Management.
- If deemed an 'eligible data breach', Building Futures Care will notify the affected individuals and report to the Office of the Australian Information Commissioner (QAIC) as required by law.

Examples:

- Lost service device.
- Unauthorised image disclosure.

CHILD PROTECTION AND ONLINE SAFETY

- Any digital content raising child safety concerns must be reported in line with mandatory reporting obligations.
- Grooming, exploitation or inappropriate digital contact must be immediately reported to relevant authorities.
- Educators must always model safe and respectful digital behaviour.
-

TRAINING AND REVIEW

- Mandatory induction training on digital device compliance.
- Annual policy review or earlier if legislation changes.
- Compliance auditing of device use.

RELEVANT LEGISLATION

- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011
- Privacy Act 1988
- Office of the Australian Information Commissioner
- Work Health and Safety Act 2011
- National Quality Standard (QA2, QA4, QA7)
- Child Safe Standards (2026)
- National Model Code for Taking Images of Children in Early Childhood Education and Care
- Proposed Regulation 2.11 Digital Technologies
- Notifiable Data Breaches Scheme (Privacy Act 1988)
- Australian Privacy Principles
- eSafety Commissioner guidance
- National Principles for Child Safe Organisations

DOCUMENT RECORD

Date Created	29/08/2025
Date reviewed	10/03/2026
Date to be reviewed	10/03/2027
Document redesign	10/04/2026
Updated to Regulation	21/05/2026