Building Futures Care Digital Technology Policy and Procedure

Purpose

This policy outlines Building Futures Care's commitment to managing digital technologies responsibly within family day care environments. 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 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, 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 strongly discouraged 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:

- 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.
- 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:

- 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,
- 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.

Permitted Use:

Only service-supplied or service-authorised devices may be used.

Images must:

- Reflect dignity and respect.
- Exclude children without written consent.
- Not include identifying details (full names, addresses, signage).
- Be permanently deleted from the device after secure upload.

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

Date Implemented: 29/08/2025

Date Reviewed: 10/03/2026

Date to be reviewed: 10/03/2028