Digital Technology Policy

Building Futures Care

Purpose

This policy outlines Building Futures Care's commitment to managing digital technologies responsibly. It ensures the protection of sensitive information and the appropriate use of digital devices, photos, videos, and data management systems. We aim to maintain the trust of families, educators, and the community through clear and respectful digital practices.

Policy Statement

Building Futures Care recognises that digital technologies are essential for communication, documentation, and record-keeping. We are committed to safeguarding personal, sensitive, and confidential information through secure and ethical use of digital tools. All educators, staff, visitors, students and volunteers must follow this policy to protect privacy and comply with legal obligations under the **Privacy Act 1988** and **Notifiable Data Breaches Scheme**.

Responsibilities

All Coordinators, Educators, Scheme Staff, Students, Volunteers, and Visitors must:

- Understand their legal and ethical obligations related to digital technology use.
- Respect the privacy and dignity of all children and families.
- Follow the procedures outlined below when using devices, storing data, or capturing media.

Procedures

Digital Information Security & Device Management

- All digital devices used for work (e.g. phones, tablets, laptops) must:
    - Have password or biometric security enabled.
    - Be kept in secure locations when not in use.
    - Never be left in vehicles or public areas unattended.
- Devices used for capturing or storing children's information, photos, or videos, must be stored securely with password access and biometric security enabled.
- Passwords must not be shared or stored insecurely.

Surveillance

- If surveillance (such as CCTV or video monitoring) is in use, families will be informed prior to or upon enrolment, and clear signage will be displayed in visible areas to indicate that surveillance is operating.
- All surveillance footage will be managed in accordance with privacy and data protection laws and used strictly for safety, security, and compliance purposes.
- Only authorised people can access recordings.
- Secure storage and destroy or de-identify data when no longer needed

---

Photographs and Videos

- During enrolment parents/carers give authorisation that the child may be photographed or videoed by educators for the purpose of documenting their learning or development, social media and marketing purposes.
- **Images, videos or content** are not inappropriately posted online or shared through other applications, including those not for the purpose of sharing with a child's family or carer.
- Devices used for capturing or storing children's information, photos, or videos, must be stored securely with password access and biometric security enabled.

- Group photos intended for sharing must exclude or obscure any children who do not have permission for their images to be shared.
- **Child Participation**: Explain consent in child-friendly terms and allow children to withdraw consent at any time
- All media must be:
    - Regularly uploaded to secure cloud storage (e.g. OneDrive).
    - Permanently deleted from devices once stored securely.

Storage and Access to Digital Information

- All sensitive digital records (e.g. enrolment forms, incident reports, health or education plans) must be stored:
    - In encrypted or password-protected digital systems.
    - With access limited to authorised personnel only.
- Families have the right to access their own digital 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 Scheme staff must not post photos or identifying information about children on personal social media accounts.
- 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.

- Participation in closed family day care social media groups is limited to families with children currently enrolled in the service. 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 iPads accessed by children in care

- Must have **written parental authorisation** before being used in the service.
- Must have **appropriate parental controls** enabled by the parent/carer before being brought to care. These should include:
    - App restrictions (age-appropriate content only),
    - Time limits,
    - Safe browsing filters,
    - Not to be used for taking photos/videos
    - **Not** share devices with others
- Educators retain the right to decline use of any personal device that does not meet safety or developmental appropriateness.
- Devices will be stored securely when not in use and will only be accessed under **active supervision**.

Notifiable Data Breaches Scheme

In the event of a suspected or actual data breach:

- It must be reported immediately to the Nominated Supervisor or Building Futures Care Management.
- Building Futures Care will assess whether the breach is likely to result in serious harm.
- If deemed an "eligible data breach," Building Futures will notify the affected individuals and report to the **Office of the Australian Information Commissioner (OAIC)** as required by law.

Examples of breaches include:

- Loss or theft of a device containing children's records.
- Sending a confidential email to the wrong recipient.
- Displaying private health or allergy information publicly without consent.

Training and Review

- All Educators and Coordinators will receive training on this policy upon commencement and as part of ongoing professional development.
- This policy will be reviewed annually or sooner if legislation changes or incidents occur.

Acknowledgements, References and Resources

Australian Government – Federal Register of Legislation. (n.d.) Privacy Act 1988. Accessed 8 July,

2019 from https://www.legislation.gov.au/Series/C2004A03712

Office of the Australian Information Commissioner. (n.d.) Notifiable Data Breaches Scheme.

Accessed 8 July, 2019 from https://www.oaic.gov.au/privacy/notifiable-data-breaches#how-to-notify

Date Implemented:
Review Date: