Safe Use of Digital Technologies and Online Environments Policy

Early Childhood Education and Care (Queensland)

Effective Date: 13/03/2026
Review Date: 13/03/2027
Quality Areas: QA2 | QA6 | QA7

Policy Category

Governance | Child Safety | Information Management

Purpose

The purpose of this policy is to ensure the safe, ethical, and responsible use of digital technologies and online environments in ways that protect children's safety, wellbeing, dignity, and privacy while supporting their learning and development.

The service recognises that digital technologies can enhance documentation, communication, and administration when used intentionally and purposefully. Robust systems are maintained to manage digital risks, prevent unauthorised recording or sharing of images, and ensure compliance with all legislative and regulatory requirements.

Scope

This policy applies to all:

- Approved Provider
- Nominated Supervisor
- Responsible Person in Charge (RPIC)
- Educators and staff (including casuals)
- Educational Leader
- Students and preservice teachers
- Volunteers

- External contractors working with children
- Families and visitors

This policy applies to the use of service-owned and personal digital devices on service premises and during service-related activities, including excursions.

Guiding Principles

- Children's safety and wellbeing are paramount
- Children's rights to dignity, privacy, and participation are upheld
- Digital technologies are used intentionally and purposefully
- Child Safe Standards are embedded in everyday practice
- Cultural safety and inclusion are respected
- Continuous improvement and accountability are prioritised

Legislative and Regulatory Framework

This policy complies with:

- Education and Care Services National Law and Regulations (Qld)
- National Quality Standard
- National Child Safe Standards
- ACECQA National Model Code for Taking Images or Videos of Children
- Privacy Act 1988 (Cth)
- Information Privacy Act 2009 (Qld)
- Online Safety Act 2021 (Cth)

Definitions

Approved Platform: A digital platform or application that has been assessed and approved by the Approved Provider for the storage, transmission, or display of children's images or personal information.

Image: Still photographs, video recordings, audio-visual recordings, screenshots, and any other digital visual representation of a child. Images of children are classified as personal information under applicable privacy legislation.

Electronic Device: Any device capable of recording, storing, sharing, or transmitting images (e.g., smartphones, smartwatches, tablets, cameras, computers).

Personal Electronic Device: Any device owned by staff, students, volunteers, or contractors.

Service-Owned Device: A tablet, camera, or other device owned and authorised by the service.

Policy Statements and Procedures

1. Service-Owned Digital Devices

- Only service-owned devices are used to photograph or document children.
- Use is intentional, developmentally appropriate, and linked to the program.
- Children's access to digital devices is directly supervised by an educator at all times.
- Devices are password-protected and records stored securely on approved platforms.

---

2. Approved Use of Images, Consent, Privacy, Storage and Security

- Images of children may only be used for the following approved purposes:
    - documenting children's learning and development;
    - communicating with families through approved platforms;
    - regulatory and compliance requirements; and
    - service promotional material, where specific written consent has been obtained.
- Images must not be used for any purpose not expressly authorised by this policy.
- Written parental consent is obtained during enrolment for the recording, use, and storage of children's images, specifying the approved purposes for which images may be used. Consent may be withdrawn by a parent or guardian at any

time by notifying the service in writing, and the service must take reasonable steps to comply with such withdrawal within five business days.

- Images must be treated as personal information and stored only on approved platforms. Images must never be stored on personal devices or external storage.
- Access is restricted to authorised staff.
- Images of children are retained only for the period necessary to fulfil the approved purpose and in accordance with the service's records retention schedule. Upon a child's departure from the service, images are securely deleted or de-identified within 90 days unless retention is required by law.

---

3. Staff Personal Digital Devices

Staff must never:

- Record or share images of children using personal devices.
- Access personal online platforms while working with children.
- Permit children to access personal devices.
- Compromise supervision through device use.

When children are present:

- Personal devices must be stored securely in staff lockers, or staff-only areas such as the teachers programming space or office.
- Personal devices must not be kept in children’s learning environments or other areas accessible to children.

Exemptions to Restrictions on Personal Device Possession

Exemptions to the restriction on possession of personal devices in centre-based services may apply in the following circumstances:

- When authorised by the Approved Provider or Nominated Supervisor.
- During excursions.
- While transporting children.
- Where it is not practicable to obtain prior authorisation and a reasonable person would consider possession necessary for:
    - Supporting a child or staff member with disability or health needs.
    - Urgent communication with family.

- Situations where service-supplied devices cease functioning.
- Emergency situations.
- Work health and safety requirements.

In all circumstances, use of a personal device must not compromise active supervision, children's safety, or privacy.

---

4. Wearable Technology

- Smartwatches, fitness trackers, or other wearable devices may be worn only if they cannot record, store, or transmit images or audio.
- Notifications must be silenced during working hours. Staff are responsible for ensuring their wearable devices comply with this requirement and must seek guidance from the Nominated Supervisor if uncertain.

---

5. Pre-Service Teachers and Practicum Students

Pre-service teachers and practicum students must complete a digital safety induction prior to commencing their placement. They must use service-owned devices only and under the supervision of an educator. Personal devices remain stored securely in staff-only areas at all times.

---

6. Visitors, Contractors and Volunteers

- All visitors, contractors, and volunteers must be informed of the service's digital safety requirements upon arrival.
- Personal devices must be stored securely and must not be used to photograph, record, or otherwise capture images of children or the service environment.
- Signage regarding these requirements must be displayed at all entry points to the service.

---

7. Family Use of Digital Devices

Families may photograph or record their own child only during designated service events (such as concerts, end-of-year celebrations, or other events specified by the service), ensuring no other children or identifying details appear in images. The service reserves the right to restrict or prohibit recording at any event if privacy or safety risks arise.

---

8. Online Environments and Digital Learning

- Children access online environments only through service-approved platforms under direct educator supervision.
- The Approved Provider or Nominated Supervisor must assess and approve all digital platforms and applications before they are introduced, having regard to data security, age-appropriateness, and compliance with applicable privacy legislation.

---

9. Safety, Child Safe Standards and Incident Response

- Digital risks are assessed as part of the service's ongoing risk management process and whenever new technologies or platforms are introduced. Incidents involving digital safety breaches are responded to promptly in accordance with the service's incident management procedures, and affected families are notified within 24 hours of the service becoming aware of the incident.
- Where an incident constitutes a serious incident, notifiable data breach, or a breach of the Child Safe Standards, the service must also report in accordance with its obligations under the Education and Care Services National Law, the *Privacy Act 1988* (Cth), and any other applicable legislation.

---

10. Staff Conduct and Accountability

- All staff comply with the ACECQA National Model Code of Conduct. Breaches are reported and managed in line with service procedures.
- Staff must not engage with families or children enrolled at the service through personal social media accounts. Any online interaction with families must occur through service-approved communication platforms only.

Roles and Responsibilities

Approved Provider / Nominated Supervisor: Governance, compliance, monitoring
Educators and Staff: Implementation and reporting
Families: Consent and respectful engagement
Children: Supported to express views and preferences

Monitoring and Review

This policy is reviewed annually or following legislative change, or after any digital safety incident.

Audits, incident analysis, and feedback inform continuous improvement.

Related Policies

- Child Protection Policy
- Privacy and Confidentiality Policy
- Code of Conduct
- Governance and Risk Management Policy

Approval

Approved Provider / Nominated Supervisor Name: _____
Signature: _____
Date: _____