Digital Technology, Images, Devices & Online Safety Policy

Purpose

Insight Early Learning is committed to ensuring the safety, wellbeing, dignity, and privacy of all children through the safe, appropriate, and purposeful use of digital technology. This policy establishes clear guidelines and procedural requirements for the safe use of technology, devices, images, and digital media across all services, and the storage and removal of digital images and recordings.

This policy supports the service's commitment to maintaining a child-safe environment by ensuring all digital technology use, image management, and online interactions prioritise children's safety, privacy, and wellbeing. Practices outlined within this policy align with supervision requirements, child protection obligations, and secure data management systems.

Scope

This policy applies to all Insight Early Learning services, children, families, and caregivers, educators, staff, and Leadership Team. It also includes volunteers, students, contractors, and visitors. It relates to all company-issued and personal electronic devices capable of capturing, storing, or sharing data.

Legislative Requirements

Education and Care Services National Regulations, particularly:	
Regulations	**Description**
Reg 155	Interactions with children
Reg 156	Relationships in groups
Reg 168	Policies and procedures
Reg 170	Policies to be followed
Reg 171	Policies to be kept available
Reg 172	Notification of change (if surveillance changes)
Reg 156	Relationships in groups

Relevant National Quality Standard (NQS) Elements

Quality Area 2 – Children's Health and Safety	
2.2.1	Supervision: Digital technology use is actively monitored to ensure children's safety at all times.
2.2.2	Incident and emergency management: Online risks, cyber safety concerns, or inappropriate content exposure are responded to promptly and effectively.
Quality Area 5 – Relationships with Children	
5.1.1	Positive educator to child interactions: Digital technology is used to support respectful, responsive, and meaningful interactions.
5.2.1	Collaborative learning: Technology is used in a way that promotes safe, inclusive, and supportive engagement between children.

DOCUMENT CONTROL					
Policy Title	Digital Technology, Images, Devices & Online Safety Policy				
Document Owner	Taylor Rhodes		**Document Author**	Angela Dorrian	
Policy Reviewed	28/04/2026	**Document Version**	V1.0	**Revision Due Date**	28/04/2027

Quality Area 7 – Governance and Leadership	
7.1.2	Management systems: Clear policies and procedures are in place for the safe, ethical, and appropriate use of digital technology, images, and devices.
7.1.3	**Roles and responsibilities:** Educators, staff, and management understand their responsibilities in relation to digital safety, privacy, and acceptable use

Legislation and Guidelines

This policy is informed by and complies with:

- **Privacy Act 1988 (Cth)**
- **Australian Privacy Principles (APPs)** – particularly in relation to the collection, use, storage, and disclosure of personal and sensitive information, including children's images and data
- **Child Safe Standards** (relevant state/territory requirements, e.g., Victoria's 11 Child Safe Standards), ensuring safe environments including online and digital contexts
- **eSafety Commissioner Guidelines**, including best practice recommendations for online safety, cyber security, and safe digital environments for children

Policy Statement

- Only Insight Early Learning issued devices may be used to capture, store, or share images/videos of children
- Personal devices are strictly prohibited in classrooms or where children are cared for.
- Technology is used only to support educational and operational outcomes
- Children's rights, dignity, and privacy are always prioritised

Implementation

Use of Technology with Children

All use of digital technology aligns with child safe practices and the service's Child Protection Policy, ensuring children are protected from harm, exploitation, and inappropriate digital exposure. Educators actively uphold children's rights, dignity, and safety, and respond to any concerns in line with child protection and mandatory reporting requirements.
Technology is used intentionally to support and enhance learning within the educational program. Educators model safe, respectful, and balanced use, ensuring all digital tools are purposeful and developmentally appropriate.
Devices are used only in visible, supervised areas, with screens positioned to enable clear monitoring and maintain a child-safe environment.
Screen time is always supervised and purposeful. Children aged two to five years have limited access in line with the *Get Up & Grow* Guidelines. Educators actively supervise technology use, pre-screen and risk assess all digital tools, promote positive digital citizenship, and maintain professional boundaries.
Internet access is supervised at all times, with secure networks and filtering systems in place. Risks associated with digital technology are assessed prior to use.

Use of Personal Devices and Digital Media

The use of personal devices, including mobile phones, tablets, smartwatches, digital cameras, laptops, or any electronic device capable of capturing or transmitting images or data (including USB drives and other storage devices), is strictly prohibited within all care environments.
Personal devices must not be used unless explicitly authorised in writing by the Approved Provider.

Approved Technology and Device Use

The use of technology within the service is strictly managed to ensure safety and security.

- Only company-issued devices are permitted for use
- All devices must be password-protected and securely maintained
- Internet access is filtered, restricted, and monitored at all times

- Access to inappropriate or non-work-related websites is blocked through network-level security controls and device management systems
- Devices must remain on site unless prior authorisation has been granted

Photography, Video and Digital Media Use

Consent, Authorisation, Refusal and Withdrawal

Written parental consent must be obtained prior to capturing any images of children. Consent is collected at enrolment and reviewed annually.

Images are captured only to support and enhance the educational program and may be used in children's learning documentation. Images may also be used for approved marketing purposes. Images must not include identifying personal information.

Families have the right to withdraw consent at any time. Withdrawal must be provided in writing. Upon receipt:

- Records are updated immediately
- All relevant staff are informed
- No further images of the child are captured

All images are:

- Stored securely on approved platforms
- Accessible only to authorised personnel
- Shared exclusively through approved systems

Images displayed within the service are presented respectfully and do not include identifying personal information.

External sharing of images occurs only where explicit written consent has been provided and must align with the service's Social Media Policy.

Where external providers (e.g. photographers, therapists, marketing agencies) are engaged:

- Specific written consent must be obtained
- Providers must comply with the service's privacy, child safety, and data protection requirements
- Clear expectations regarding storage, use, and deletion of images must be established

Exceptions to Restrictions

Exceptions to the restriction on personal device use may be granted in limited and exceptional circumstances. All exceptions must be approved in writing by the Approved Provider or their delegate.

Exceptions may include:

- Emergencies (e.g. lockdowns, evacuations, serious incidents, or lost children)
- Personal health, disability, or accessibility needs
- Urgent family circumstances
- Temporary failure of a service-issued device
- Approved access for community members or stakeholders for specific business purposes

Approval requests submitted to compliance@insightel.com.au with:

Date of Request	
Service	
Staff Member who is requesting the approval	
Purpose of Exception	
Device Type	
Child/Individual involved (If applicable)	
Period of Approval needed (Start and Finish)	
Name of person approved	

Personal devices are never authorised for capturing/storing children's images.

Image and Device Management

All digital images, including videos:

- Must be uploaded to approved platforms
- Must be deleted from service devices within three (3) months

Automated deletion processes ensure all remaining content is removed at least every six (6) months.

Devices are subject to quarterly audits conducted by Centre Directors, with compliance monitored and recorded through Safety Culture.

To ensure data security across the device lifecycle, all devices must undergo a factory reset prior to reassignment or disposal.

Incident Response

Any unauthorised images must be deleted immediately.

An incident report must be completed, and all relevant regulatory processes followed, including notification to appropriate authorities where required. All incidents must be reported to the Centre Director and Compliance team.

The service adopts a proactive approach to data protection. Any suspected or actual:

- Data breach
- Unauthorised access
- Disclosure of personal information

is immediately escalated, documented, and managed in accordance with privacy legislation and organisational procedures. This includes notification to affected individuals and relevant authorities where required.

Continuous monitoring and review processes are implemented to strengthen data security and prevent future breaches.

CCTV and Surveillance

Insight Early Learning utilises CCTV to support safety, security, and incident management.

- Cameras are installed only in appropriate, non-private areas
- Clear signage is displayed to inform all stakeholders
- Footage is accessed only by authorised personnel
- Footage is used solely for legitimate safety, security, or legal purposes
- All footage is stored securely and retained for a limited period in accordance with organisational requirements and the Privacy Act 1988

Compliance

Non-compliance with this policy, including misuse of technology or failure to adhere to procedures, may result in disciplinary action in accordance with organisational policies and procedures.

Review

All educators, staff, and relevant stakeholders participate in ongoing training and professional development to ensure a strong understanding of digital safety, privacy, and appropriate technology use. This includes induction, regular policy refreshers, and updates aligned with legislative and best practice changes. This policy will be reviewed annually or as legislation and best practice changes, with a commitment to continuous improvement and maintaining a safe, secure, and child-focused digital environment.

DOCUMENT CONTROL					
Policy Title	Digital Technology, Images, Devices & Online Safety Policy				
Document Owner	Taylor Rhodes		**Document Author**	Angela Dorrian	
Policy Reviewed	28/04/2026	**Document Version**	V1.0	**Revision Due Date**	28/04/2027