CHILD SAFETY & PROTECTION:

SAFE USE OF DIGITAL TECHNOLOGIES AND ONLINE ENVIRONMENTS

PURPOSE

This policy provides clear guidelines for the safe, appropriate and responsible use of digital technologies and online environments at Essential Early Learning. We are committed to protecting children's privacy, dignity and safety in both physical and digital spaces, whilst harnessing the educational benefits of technology.

Our service will:

- Ensure children's privacy and dignity are protected when using digital technologies
- Obtain appropriate consent for taking, using and storing images/videos of children
- Use digital technologies safely and appropriately to support children's learning
- Protect children's personal information in accordance with privacy legislation
- Ensure online environments are child safe and secure
- Guide children in developing safe and responsible digital citizenship

---

SCOPE

This policy applies to:

- All children enrolled at the service
- The approved provider, nominated supervisor, educators and staff
- Students on placement, volunteers and contractors
- Parents, guardians and families
- All digital technologies owned, used or accessed by the service
- All online platforms, websites, applications and communication tools used by the service

---

LEGISLATIVE REQUIREMENTS

This policy is based on the following legislation and standards:

Education and Care Services National Law Act 2010

- Section 167: Offence relating to protection of children from harm and hazards
- Section 170: Offence relating to unauthorised persons on education and care service premises

Education and Care Services National Regulations 2011

- Regulation 168: Education and care service must have policies and procedures
- Regulation 181: Confidentiality of records kept by approved provider
- Regulation 183: Storage of records and other documents

National Quality Standard

- Quality Area 2: Children's Health and Safety

- Element 2.2.1: At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard
- Quality Area 6: Collaborative Partnerships with Families and Communities
- Element 6.1.1: Families are supported from enrolment to be involved in the service and contribute to service decisions

NSW and Commonwealth Legislation:

- Privacy Act 1988 (Commonwealth)
- Australian Privacy Principles (APPs)
- Privacy and Personal Information Protection Act 1998 (NSW)
- Children's Guardian Act 2019 (NSW) - Child Safe Standards (Standard 8)
- Surveillance Devices Act 2007 (NSW)
- Work Health and Safety Act 2011 (NSW)
- Spam Act 2003 (Commonwealth)
- Copyright Act 1968 (Commonwealth)

KEY DEFINITIONS

Digital Technology: Any electronic device, tool or platform used to create, store, share or access information. This includes computers, tablets, smartphones, cameras, digital learning tools, and online platforms.

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable, including name, image, video, address, date of birth, medical information, and other identifying information.

Consent: Informed, voluntary agreement given by a parent/guardian for a specific purpose. Consent must be current, specific, informed and freely given.

Social Media: Online platforms and applications that enable users to create, share and exchange content, including Facebook, Instagram, Twitter, YouTube, and similar platforms.

Surveillance Device: A device used to monitor, record or observe persons or activities, including CCTV cameras, audio recording devices, and other monitoring equipment.

Online Environment: Any digital space or platform accessed via the internet, including websites, applications, learning platforms, and communication tools.

POLICY PROCEDURES

1. Taking, Using and Storing Images and Videos of Children

When Images/Videos May Be Taken:

The service may take photographs or videos of children for the following purposes:

- Documentation of children's learning and development
- Creating individual learning portfolios
- Display within the service to celebrate children's experiences
- Communication with families about their child's day
- Service promotional materials (with specific consent)
- Social media and website content (with specific consent)

- Educational and training purposes

Guidelines for Taking Images/Videos:

- Only service-owned devices (iPad) will be used to photograph or record children
- Personal mobile phones or devices must not be used to photograph children
- Children must be appropriately dressed (no images during nappy changes, toileting, or sleep time unless for specific developmental documentation with parental consent)
- Images must be respectful of children's dignity
- Focus on the activity or learning experience rather than close-up facial images where possible
- Avoid images that could be misinterpreted or misused
- Check consent records before including children in photographs
- Children without consent must not be identifiable in group photos

Storage of Images/Videos:

- All images and videos will be stored securely on password-protected devices or secure servers
- Images will be backed up regularly to prevent loss
- Access to stored images is restricted to authorised staff only
- Images must not be stored on personal devices
- Cloud storage services used must have appropriate security and privacy protections
- Images and videos will be organised by child and date for easy retrieval

Use of Images/Videos:

Images and videos may only be used for purposes specified in the enrolment form or consent form:

- Internal use (portfolios, displays within the service, documentation)
- External use (promotional materials, website, social media, publications) - requires specific consent
- Images will not be used for purposes beyond the scope of consent provided
- If consent is withdrawn, images will no longer be used (though already published materials may remain until practical to remove)

Destroying Images/Videos:

- Images included in a child's records will be retained as per record retention requirements (until child turns 25)
- Images not included in official records will be deleted within 12 months of being taken, or when consent is withdrawn
- When a child leaves the service, images not included in handover portfolios will be securely deleted
- Deletion must be permanent and irreversible (not just moved to recycle bin)
- Physical photographs will be shredded or returned to families

2. Obtaining Parent Authorisations for Images and Videos

Consent Requirements:

Written consent from parents/guardians is required before taking, using, or publishing images or videos of children. Consent must be:

- Informed: Parents understand what they are consenting to
- Specific: Separate consent for different uses (internal vs external)

- Current: Consent is reviewed annually or when circumstances change
- Freely given: Parents can refuse or withdraw consent without consequence
- In writing: Documented and signed in enrolment form

Types of Consent:

The service will obtain separate consent for:

- General photography/videography for internal use (portfolios, displays, documentation)
- Use of images in promotional materials (brochures, flyers)
- Publication on the service website
- Publication on social media platforms
- Use in media releases or publications
- Use of child's name alongside images

Consent Process:

- Consent will be obtained at enrolment
- Parents will be clearly informed about how images will be used
- Parents can consent to some uses and not others
- Consent will be reviewed annually
- Parents may withdraw or modify consent at any time
- Consent records will be kept in the child's file

Withdrawing Consent:

- Parents may withdraw consent at any time by notifying the service in writing
- Following withdrawal, no new images of the child will be taken or used
- Existing images will be removed from displays and future publications
- Images already published online or in print may remain until practical to remove
- Images in the child's portfolio or records will be retained as per record requirements

3. Use of Surveillance Devices (CCTV)

Purpose of CCTV:

The service may use CCTV cameras for the following purposes:

- Ensuring children's safety and security
- Monitoring service operations and quality
- Investigating incidents or complaints
- Providing evidence in case of emergencies or disputes
- Deterring inappropriate behaviour
- Protecting staff from false allegations

CCTV Installation and Operation:

As CCTV is used, the following requirements apply:

- CCTV is only be installed in common areas (playrooms, outdoor areas, entry/exit points)
- CCTV is NOT installed in private areas (toilets, nappy change areas, sleep rooms)
- Clear signage will be displayed notifying that CCTV is in operation
- Families will be informed about CCTV use during enrolment
- CCTV will operate continuously during service hours
- Audio recording will only occur if legally permissible and families are clearly informed

Access to CCTV Footage:

- Access to live CCTV feeds is restricted to the approved provider and nominated supervisor
- Recorded footage is stored securely with password protection
- Only authorised personnel may view recorded footage
- Parents do not have automatic access to view CCTV footage
- Footage may be viewed in specific circumstances: investigating incidents, responding to complaints, legal requirements, regulatory authority requests

Storage and Deletion of Footage:

- CCTV footage will be stored for a maximum of 7 days on the CCTV modem, footage retained further if required to download for investigation or legal purposes
- After 7 days, footage will be automatically overwritten unless retained for specific purposes
- Footage related to incidents or investigations will be retained until the matter is resolved
- Footage will be stored securely on encrypted devices or servers
- When deleted, footage will be permanently destroyed

Privacy Considerations:

- CCTV use will comply with the Privacy Act 1988 and Surveillance Devices Act 2007 (NSW)
- CCTV will not be used to monitor staff performance (except for child safety purposes)
- Footage will not be shared publicly or used for purposes other than stated
- The privacy of all individuals captured on CCTV will be respected

4. Use of Digital Devices Issued by the Service

Service-Owned Devices:

The service may provide the following digital devices for educational and administrative purposes:

- Tablets for children's learning and documentation
- Cameras for photographing children's activities
- Computers for planning, documentation and communication
- Smart devices for communication with families

Acceptable Use:

Service-issued digital devices may only be used for:

- Educational purposes with children
- Documentation of children's learning
- Communication with families about children's experiences
- Service administration and planning
- Professional development and research
- Accessing approved educational content and resources

Prohibited Use:

Service devices must NOT be used for:

- Personal social media (except service accounts)
- Personal email or messaging
- Personal photography or video recording
- Online shopping or banking

- Accessing inappropriate content
- Downloading unauthorised software or applications
- Any illegal activities

Security Requirements:

- All devices must be password protected
- Passwords must be strong and kept confidential
- Devices must not be left unattended while unlocked
- Devices must be stored securely when not in use
- Lost or stolen devices must be reported immediately
- Anti-virus software must be kept up to date
- Software updates must be installed promptly

Personal Mobile Phones and Devices:

- Staff personal mobile phones must be stored in lockers or bags during work hours
- Personal devices must not be used in areas where children are present
- Personal devices must never be used to photograph or record children
- Emergency personal calls can be made/received in the office
- Smartwatches must not be used to photograph or record children

5. Children's Use of Digital Devices

Educational Use of Technology:

Children may use digital technologies as part of their learning program:

- Tablets for educational games and applications
- Computers for age-appropriate learning activities
- Digital cameras to document their own learning and experiences
- Interactive whiteboards or smart boards
- Age-appropriate programmable toys (e.g., Bee-Bots)
- Audio recording devices for storytelling and music

Supervision and Safety:

- Children's use of technology will always be supervised by educators
- Devices will be positioned where educators can see screens
- Internet access will be filtered and monitored
- Only age-appropriate, pre-approved content and applications will be accessible
- Children will be taught safe and respectful use of technology
- Screen time will be balanced with other learning experiences

Teaching Digital Citizenship:

Educators will teach children age-appropriate concepts including:

- Taking turns and sharing digital devices
- Being kind and respectful online
- Caring for digital equipment
- Basic concepts of online safety appropriate to their age
- Not sharing personal information
- Telling a trusted adult if something makes them uncomfortable

Screen Time Guidelines:

- Screen time will be intentional, purposeful and curriculum-linked
- Technology is a tool to support learning, not a substitute for active play
- Screen time will be limited and balanced with other activities
- Passive screen time (watching videos) will be minimal
- Interactive, creative and collaborative uses of technology will be prioritised

6. Online Environments and Communication Platforms

Service Website:

- The service website will contain general information about the service
- No personal information about children will be published without consent
- Images on the website will only include children whose parents have provided specific consent
- Children's full names will not be used alongside images

Social Media:

If the service maintains social media accounts:

- Only designated staff will have access to service social media accounts
- All posts will be professional and appropriate
- Children's images will only be posted with specific parental consent
- Children's full names will not be used
- Comments will be moderated
- Privacy settings will be regularly reviewed
- Staff personal social media must not mention the service or post images of children

Communication Platforms:

The service may use secure online platforms for communication with families:

- Communication app OWNA
- Email for formal communications
- SMS for urgent messages
- All platforms used must have appropriate privacy and security features
- Parents will be informed about which platforms are used and how
- Personal information will only be shared on secure platforms

Online Safety:

- All online platforms will have secure login credentials
- Passwords will be strong and changed regularly
- Data will be encrypted where possible
- Privacy settings will be set to maximum
- Software will be kept up to date
- Data breaches will be reported to affected families and authorities as required

7. Privacy and Data Protection

Privacy Principles:

The service will comply with the Australian Privacy Principles (APPs) including:

- Only collecting personal information that is necessary

- Using and disclosing information only for the purpose collected
- Storing information securely
- Providing individuals with access to their information
- Correcting information when requested
- Destroying or de-identifying information when no longer needed

Data Security:

- All digital information will be stored securely
- Access will be restricted to authorised personnel only
- Regular backups will be performed
- Firewalls and antivirus software will be maintained
- Devices will be encrypted where possible
- Staff will be trained in data security practices

EDUCATOR AND STAFF RESPONSIBILITIES

Nominated Supervisor/Person in Day-to-Day Charge:

- Ensure all staff understand and comply with this policy
- Maintain consent records and ensure they are current
- Monitor compliance with image and video procedures
- Oversee security of digital devices and data
- Manage CCTV systems (if applicable)
- Ensure privacy breaches are reported and managed
- Review and approve content before online publication

All Educators and Staff:

- Follow this policy at all times
- Only photograph/record children with consent
- Use only service-owned devices for photographing children
- Store personal devices securely away from children
- Supervise children's use of technology
- Use service devices responsibly and appropriately
- Protect passwords and login credentials
- Report any privacy or security concerns
- Respect children's privacy and dignity

FAMILY RESPONSIBILITIES

Families are responsible for:

- Reading and understanding this policy
- Providing informed consent for images and videos
- Reviewing and updating consent annually
- Informing the service if they wish to withdraw or modify consent
- Not photographing or recording other children without consent
- Not posting images of other children on social media
- Using service communication platforms appropriately
- Keeping login credentials secure

- Reporting any concerns about digital safety or privacy

RELATED POLICIES AND PROCEDURES

- Privacy and Confidentiality Policy
- Providing a Child Safe Environment Policy
- Interactions with Children Policy
- Enrolment and Orientation Policy
- Code of Conduct
- Social Media Policy

REFERENCES AND RESOURCES

- ACECQA: Guide to the National Quality Framework
- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011
- National Quality Standard
- Australian Children's Education and Care Quality Authority (ACECQA) website: www.acecqa.gov.au
- Privacy Act 1988 (Commonwealth)
- Australian Privacy Principles
- Office of the Australian Information Commissioner (OAIC): www.oaic.gov.au
- Privacy and Personal Information Protection Act 1998 (NSW)
- Surveillance Devices Act 2007 (NSW)
- eSafety Commissioner: www.esafety.gov.au
- Office of the Children's Guardian (NSW): www.ocg.nsw.gov.au
- Children's Guardian Act 2019 (NSW) - Child Safe Standard 8
- Copyright Act 1968 (Commonwealth)

POLICY REVIEW

This policy will be reviewed every two years or more frequently if required due to:

- Legislative changes
- Changes in technology or digital platforms used
- Changes in best practice or eSafety guidance
- Privacy breaches or incidents
- Feedback from families, educators or staff
- Following regulatory assessment and rating
- Updates from the eSafety Commissioner or privacy regulators

Date policy was last reviewed: 11/01/2026
Date for next review: 11/01/2028
Reviewed by: Director and Staff