ACCEPTABLE USE OF CCTV IN EDUCATION & CARE SETTINGS

1. Policy statement

Weldon Children's Services places child safety at the centre of everything we do. We ensure that every reasonable precaution is taken to protect the children attending our services from harm and hazard. We have comprehensive processes in place for managing authorisations that are sensitive to the needs of children and their families. We ensure digital technologies such as Closed-Circuit Television (CCTV) are used ethically, securely, and in alignment with child protection, privacy legislation, and sector standards. This policy supports safe learning environments, protects personal data, and promotes trust among children, families, and educators.

CCTV surveillance is used solely for the purposes of:

- Enhancing the safety and security of children, educators, staff, and visitors
- Protecting service property and assets
- Assisting in the investigation of incidents or allegations
- Maintaining compliance with regulatory requirements

2. Background

The Education and Care Services National Regulations require approved providers to ensure their services have policies and procedures in place in relation to the acceptable use of digital technology, devices and media in education and care settings. Children's safety and wellbeing is of primary importance, and Weldon Children's Services ensures that appropriate measures are in place to protect children from any harm or hazard. Safeguarding children during their time in the service is enabled by the implementation of policies and procedures. CCTV recording also records images of educators, employees, families, students, volunteers, approved contractors, and authorised visitors.

3. Scope of this policy

This policy applies to:

- The Approved Provider and Persons with Management or Control
- Nominated Supervisor and all educators
- Staff, students, volunteers, and contractors
- Families and visitors to the service
- All areas where CCTV cameras are installed

RELEVANT LEGISLATION AND STANDARDS

National Quality Framework

- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011: Regulations 12, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 181, 183, 184
- National Quality Standard, Quality Area 2: Children's Health and Safety
- National Quality Standard, Quality Area 7: Governance and Leadership

Privacy Legislation

- Privacy Act 1988 (Cth) and Australian Privacy Principles
- State/Territory surveillance legislation (as applicable):
    - Surveillance Devices Act 2007 (NSW)
    - Surveillance Devices Act 1999 (Vic)
    - Invasion of Privacy Act 1971 (Qld)
    - Surveillance Devices Act 1998 (WA)
    - Surveillance Devices Act 2016 (SA)
    - Listening Devices Act 1991 (Tas)
    - Listening Devices Act 1992 (ACT)
    - Surveillance Devices Act 2007 (NT)

Other Relevant Legislation

- Work Health and Safety Act 2011
- Child Protection legislation (state/territory specific)
- Fair Work Act 2009

DEFINITIONS

CCTV (Closed Circuit Television): A video surveillance system that uses cameras to transmit signals to a specific, limited set of monitors or recording devices.

Approved Provider: The entity legally responsible for the service under the National Law.

Nominated Supervisor: The person appointed by the Approved Provider to manage the day-to-day operations of the service.

Privacy Impact Assessment: An assessment of how personal information is handled to ensure compliance with privacy obligations.

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Covert Surveillance: Surveillance conducted without the knowledge of those being observed.

POLICY DETAILS

1. PURPOSES OF CCTV USE

CCTV systems at this service are installed and operated for the following legitimate purposes:

Primary Purposes:

- To enhance the safety and security of children, educators, staff, and visitors
- To deter and detect incidents of theft, vandalism, or trespass
- To assist in managing emergency situations
- To provide evidence in the event of incidents, accidents, or allegations
- To monitor compliance with service policies and procedures
- To support quality improvement processes

CCTV will NOT be used for:

- Routine performance monitoring of staff
- Monitoring educators' break areas or private spaces
- Recording audio conversations (audio recording is not permitted)
- Covert surveillance (except in exceptional circumstances with legal advice)

2. CAMERA LOCATIONS AND COVERAGE

Permitted Camera Locations:

- Building entry and exit points
- Outdoor play areas
- Indoor learning environments (where consistent with privacy considerations)
- Reception areas
- Hallways and corridors
- Car parks and external boundaries
- Storage areas containing valuable equipment

Prohibited Camera Locations:

- Toilets and nappy change areas
- Staffrooms and designated break areas
- Areas where staff may breastfeed or express milk
- Areas where personal or confidential discussions regularly occur
- Any area where individuals have a reasonable expectation of privacy

Camera Specifications:

- Cameras will be clearly visible and appropriately positioned
- Cameras will not record audio
- Cameras will be positioned to minimize inadvertent capture of neighbouring properties
- Camera angles will be regularly reviewed to ensure appropriate coverage

3. PRIVACY CONSIDERATIONS

The service recognizes the need to balance security with privacy rights:

Privacy Impact Assessment:

- A Privacy Impact Assessment has been conducted and will be reviewed annually
- The assessment considers the impact on children's privacy and dignity
- Alternative security measures have been considered
- The necessity and proportionality of surveillance has been evaluated

Privacy Protections:

- Only the minimum amount of surveillance necessary is conducted
- Cameras are positioned to respect individual privacy
- Footage is only accessed for legitimate purposes
- Strict access controls are in place
- Retention periods are minimized
- Regular reviews ensure ongoing compliance

Children's Privacy:

- Consideration is given to children's privacy and dignity
- Cameras in learning environments are positioned to observe safety while respecting children's privacy
- Footage of children in vulnerable situations (e.g., during toileting, nappy changes) is never recorded
- Parents/guardians are informed about CCTV surveillance through enrollment processes

4. NOTIFICATION AND SIGNAGE

All individuals entering the service will be informed of CCTV surveillance:

Signage:

- Clear, prominent signage is displayed at all entry points
- Signs indicate that CCTV surveillance is in operation

- Signs include contact details for privacy inquiries
- Signs are visible and legible

Information to Families:

- Information about CCTV surveillance is included in the service handbook
- Details are provided during the enrollment process
- Parents/guardians are informed of the purposes, locations, and access procedures
- Families are notified of any changes to CCTV operations

Information to Staff:

- All staff, students, volunteers, and contractors are informed of CCTV surveillance
- Information is provided during induction processes
- Staff are aware of their rights regarding CCTV footage
- Regular reminders are provided during staff meetings

Information to Visitors:

- Visitors are informed via signage and verbally where appropriate
- Visitor sign-in procedures include acknowledgment of CCTV surveillance

5. ACCESS TO CCTV FOOTAGE

Authorized Personnel:

Access to live CCTV feeds and recorded footage is restricted to:

- Approved Provider or delegated representative
- Nominated Supervisor
- [Other specified positions with legitimate need]

Access Controls:

- Secure login credentials (unique usernames and strong passwords)
- Multi-factor authentication where available
- Access logs maintained for all viewing and downloading of footage
- Regular audits of access logs

Access Procedures:

Routine Monitoring:

- Live feeds may be monitored for security purposes
- Monitoring must be conducted professionally and respectfully

- Any concerns identified must be documented

Incident Investigation:

- Footage may be reviewed following incidents, accidents, or allegations
- Access must be documented including: date, time, person accessing, reason for access
- Only relevant footage segments are reviewed
- Independent witnesses should be present where possible

Access Requests:

Access requests from individuals or external parties will be managed as follows:

Requests from Individuals (APPs 12 & 13):

- Individuals may request access to footage containing their own image
- Requests must be made in writing
- Identity verification is required
- Response provided within 30 days
- Access may be refused if it would unreasonably impact others' privacy
- Redaction of third parties' images may be necessary

Requests from Parents/Guardians:

- Parents may request footage relating to their child
- Requests must relate to specific incidents or concerns
- The service will balance parental rights with privacy of others
- Footage showing only the requesting family's child will be provided where possible

Requests from Regulatory Authorities:

- ACECQA, regulatory authorities, and law enforcement may request footage
- Requests should be in writing (except in emergencies)
- Legal advice may be sought before release
- Release is documented

Requests from Legal Representatives:

- Requests must be accompanied by appropriate legal authority
- Legal advice will be sought before release
- Confidentiality and privacy of all parties will be considered

6. STORAGE AND RETENTION

Storage Security:

- Footage is stored on secure, encrypted systems
- Storage systems are password-protected
- Regular backups are conducted
- Physical security of storage devices is maintained
- Cloud storage (if used) complies with Australian data sovereignty requirements
- Recordings are protected through rigorous access controls

Retention Period:

Footage is routinely retained for 90 days. After this period, footage is automatically overwritten unless:

- Preserved for incident investigation
- Subject to an access request
- Required for legal proceedings
- Preserved by regulatory direction

Extended Retention:

- Footage related to incidents is retained until the matter is resolved
- Documentation justifies extended retention
- Extended retention is reviewed regularly
- Footage is securely destroyed when no longer required

Secure Destruction:

- Footage no longer required is securely deleted/destroyed
- Deletion is irreversible and complete
- Destruction is documented
- Third-party destruction services (if used) provide certification

7. SECURITY OF CCTV SYSTEMS

Technical Security:

- Systems are protected by firewalls and encryption
- Software and firmware are regularly updated
- Default passwords are changed immediately
- Systems are isolated from public networks where possible
- Regular security assessments are conducted

Physical Security:

- Recording equipment is stored in secure, locked locations
- Access to equipment is restricted
- Cameras are positioned to prevent tampering
- Regular maintenance ensures system integrity

Cybersecurity:

- Systems comply with current cybersecurity best practices
- Vulnerability assessments are conducted regularly
- Incident response procedures are in place
- Third-party security services are engaged where necessary

8. BREACH MANAGEMENT

Data Breach Response:

In the event of unauthorized access to CCTV footage:

1. Immediate Actions:

- Contain the breach and secure systems
- Assess the extent and impact
- Document all details
- Notify the Approved Provider and Nominated Supervisor

2. Assessment:

- Determine if the breach is likely to result in serious harm
- Consider sensitivity of footage and number of individuals affected
- Evaluate risk to children, families, and staff

3. Notification:

- Notify affected individuals if likely to result in serious harm
- Notify the Office of the Australian Information Commissioner (OAIC) if required
- Notify regulatory authority (ACECQA/state regulatory authority)
- Document all notifications

4. Remedial Actions:

- Implement measures to prevent recurrence
- Review and update security measures
- Provide support to affected individuals

- Review and update this policy if necessary

9. COMPLIANCE AND ACCOUNTABILITY

Responsibilities:

Approved Provider:

- Ensure CCTV systems comply with all legal requirements
- Approve CCTV policy and any amendments
- Ensure adequate resources for compliant operations
- Oversee privacy impact assessments
- Ensure staff training and awareness
- Review incident reports and breaches

Nominated Supervisor:

- Implement this policy in daily operations
- Ensure signage is current and visible
- Manage access requests appropriately
- Maintain access logs and documentation
- Report breaches or concerns to Approved Provider
- Ensure staff understand and follow procedures
- Coordinate with regulatory authorities as required

All Staff:

- Understand and comply with this policy
- Respect privacy of children, families, and colleagues
- Report any concerns about CCTV misuse
- Maintain confidentiality of footage and related information
- Only access CCTV systems if authorized

Regular Reviews:

This policy will be reviewed annually or following:

- Significant incidents or breaches
- Changes to legislation or regulations
- Changes to CCTV systems
- Recommendations from regulatory authorities
- Stakeholder feedback

Documentation:

The service will maintain:

- CCTV policy (this document)
- Privacy Impact Assessment
- Signage and notification records
- Access logs
- Incident reports
- Access requests and responses
- Training records
- System maintenance records
- Review documentation

10. COMPLAINTS AND CONCERNS

Raising Concerns:

Individuals with concerns about CCTV surveillance should:

1. Speak with the Nominated Supervisor or Approved Provider

2. Submit a written complaint through the service's complaints procedure

3. Contact the Office of the Australian Information Commissioner (OAIC): 1300 363 992 or www.oaic.gov.au

4. Contact the relevant state/territory regulatory authority

Complaints Handling:

- All complaints will be treated seriously and confidentially
- Complaints will be acknowledged within [3] business days
- Investigation will be completed within [14] days where possible
- Outcome will be communicated to the complainant
- Corrective actions will be implemented if required
- Complaints will be documented and reviewed for systemic issues

11. TRAINING AND AWARENESS

Staff Training:

All staff will receive training on:

- This CCTV policy and procedures
- Privacy obligations and principles

- Appropriate access and use of footage
- Responding to access requests
- Breach reporting procedures
- Children's privacy rights

Training Schedule:

- Induction training for all new staff
- Annual refresher training for all staff
- Additional training following policy updates
- Training records maintained

Ongoing Awareness:

- Policy available to all staff at all times
- Regular reminders during staff meetings
- Updates communicated promptly
- Questions and concerns welcomed

12. SPECIAL CIRCUMSTANCES

Emergency Situations:

- In emergencies (e.g., missing child, immediate danger), CCTV footage may be accessed immediately
- Emergency services may be granted immediate access
- Documentation to follow as soon as practicable
- Regular protocols apply once emergency has passed

Regulatory Inspections:

- Regulatory authorities will be granted access to footage during inspections if requested
- Cooperation with investigations is mandatory
- Legal advice may be sought if concerns arise

Court Orders and Subpoenas:

- Legal advice will be sought upon receipt
- Compliance is mandatory where legally required
- Privacy of individuals will be advocated for where possible

POLICY REVIEW

Review Schedule:

- Annual review by Approved Provider and Nominated Supervisor
- Consultation with staff and families
- Review of Privacy Impact Assessment
- Assessment of compliance with current legislation
- Consideration of any incidents or breaches
- Updates to reflect best practice

Version Control:

Policy version: 1.0.0

Review date: 02/26

Next review: 02/27

FURTHER INFORMATION AND SOURCES

- ACECQA: www.acecqa.gov.au
- Office of the Australian Information Commissioner: www.oaic.gov.au
- Australian Privacy Principles: www.oaic.gov.au/privacy/australian-privacy-principles
- Privacy Act 1988: www.legislation.gov.au
- State/territory regulatory authorities
- Relevant state/territory surveillance legislation