

Innsworth Preschool CCTV Policy

Last Updated: 1st January 2026

1. Purpose and Scope

1.1 Overview: This policy sets out how Innsworth Preschool uses Closed Circuit Television (CCTV) as a proportionate and legally compliant tool to promote the safety of children, staff, and visitors, and to protect preschool property.

1.2 Objective: To ensure transparency, privacy, and strict adherence to data protection laws in our surveillance practices.

2. Legal and Statutory Framework

2.1 Compliance: Our use of CCTV is governed by and complies with the following key legislation and guidance:

- The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- ICO Guidance on Video Surveillance (including CCTV) and UK GDPR.
- The Statutory Framework for the Early Years Foundation Stage (EYFS).
- The Human Rights Act 1998 (Right to a private life).
- Best Practice Principles: We apply relevant principles of vigilance and professional curiosity from *Keeping Children Safe in Education (KCSIE)* where applicable.

3. Core Principles

3.1 Approach:

- **Proportionality:** CCTV is only used in a way that is proportionate to the specific issues it is designed to address.
- **Transparency:** We are open and transparent about our use of CCTV with staff, parents, and visitors.
- **Privacy:** The system is designed and operated to respect the privacy of individuals and is never used for intrusive monitoring.
- **Audio Recording:** To maintain proportionality and comply with ICO standards, the audio recording function of the CCTV system is strictly disabled at the system level. This is verified at installation and during termly system checks, which are recorded in the maintenance log.

4. Lawful Basis for Processing

4.1 Legal Basis (UK GDPR): Our primary lawful basis for processing CCTV data is **Article 6(1)(f)**

Legitimate Interests:

- To protect the property, staff, and children of the preschool.
- To detect and prevent crime.
- To support the safety of the site.

4.2 Assessments: A formal **Legitimate Interests Assessment (LIA)** is conducted and reviewed alongside our **Data Protection Impact Assessment (DPIA)**.

- **DPIA Requirement:** A DPIA is completed prior to installation or activation and is reviewed at least annually, or whenever camera siting, coverage, retention, access, or processor arrangements change.

5. Lawful Purpose of CCTV Use

5.1 Purposes: CCTV is used only for the following specified, explicit, and legitimate purposes:

- To deter and detect crime such as trespass, theft, or vandalism.
- To support the safeguarding of children and staff by monitoring access to the premises.
- To review specific incidents involving health, safety, or safeguarding concerns.
- To protect the physical integrity of our building and property.

5.2 Limitations:

- **Performance Monitoring:** CCTV is **not** used for routine staff performance monitoring. Footage may be reviewed where necessary to investigate a specific incident or allegation (e.g., safeguarding, health and safety, security), subject to strict access controls and logging.
- **Live Viewing:** We do not provide live CCTV access to parents or third parties, and we do not routinely share footage. Footage is reviewed or disclosed only for the purposes set out in this policy.

6. Siting of Cameras and Signage

6.1 Locations: Cameras are installed only in appropriate, risk-assessed locations.

- **Internal Schedule:** A camera location schedule is maintained internally.
- **Prohibited Areas:** CCTV is strictly prohibited in areas with a high expectation of privacy, such as toilets, changing facilities, or intimate care areas.

6.2 Privacy Measures: Cameras are angled to minimize capture beyond the site boundary. Privacy masking is applied digitally to neighbouring properties or public highways where necessary.

6.3 Transparency and Signage:

- **Signage:** Clear signage is displayed at the site entrance and other prominent locations, informing all persons that CCTV is in operation and providing contact details for the data controller.
- **Privacy Notice:** Signs are supplemented by our CCTV Privacy Notice, which details purposes, lawful basis, retention, rights, and how to exercise them.

6.4 Staff Consultation: We consult and inform staff about CCTV use, locations, purposes, access controls, and retention to ensure they are aware of the surveillance environment.

7. Data Storage, Retention, and Access

7.1 Storage: Footage is stored securely on encrypted systems (e.g., local hard drive or secure cloud).

- **Processors:** We procure systems that support compliance (e.g., redaction tools). Any third-party processor (installer or cloud provider) operates under a written contract with UK GDPR-compliant terms.

7.2 Retention: Footage is retained for the minimum necessary period for the stated purposes, typically a maximum of **28 days**, after which it is securely overwritten automatically.

- **Review:** This retention period is reviewed at least annually through the DPIA.
- **Extensions:** Retention beyond the default period requires written justification (e.g., ongoing police investigation or legal proceeding), a set review date, and automatic deletion once the specific purpose ends.

7.3 Access Control:

- **Authorised Persons:** Access to live and recorded footage is strictly limited to the **Preschool Manager** and the **Designated Safeguarding Lead (DSL)**.
- **Emergency Protocol:** In their absence, named deputies may access footage only under a strictly defined emergency protocol (e.g., immediate threat to life).
- **Logging:** All instances of access (viewing or exporting) are logged in an access register (recording who, when, and the purpose). These logs are audited annually by the Whistleblowing Officer.

7.4 Export and Disclosure:

- **Security:** Exports are encrypted and password-protected.
- **Sharing:** Footage is shared only where necessary (e.g., Police, Children's Social Care, insurers) and only via approved secure transfer methods.
- **Logging:** Every disclosure is logged, recording what was shared, the reason, who authorised it, the recipient, and the date.

8. Subject Access Requests (SARs)

8.1 Rights: Individuals (including staff and parents on behalf of their children) have a right to request footage featuring themselves or their child.

8.2 Process:

- **Request Details:** Requests must, where possible, specify the date, approximate time, and location to assist us in locating the footage.
- **Preservation:** Upon receipt of a request, we will preserve relevant footage to prevent routine deletion while the request is processed.
- **Redaction:** We are legally required to redact (blur or obscure) all other individuals (third parties) in provided footage to protect their privacy. We will not provide unredacted footage showing other children, parents, or staff.
- **Limitations:** Where third-party rights would be adversely affected and effective redaction is not possible, we may lawfully limit or refuse disclosure, explaining the reasons.

- **Children's Rights:** We recognize children as data subjects. The best interests of the child are considered before any disclosure.

8.3 Timescales and Fees:

- **Timing:** Requests are processed within **one calendar month** of receipt and identity verification. This may be extended in limited, complex cases.
- **Fees:** The default position is no charge. We may only charge a reasonable fee if a request is manifestly unfounded or excessive.

9. Monitoring and Support

9.1 Awareness: Staff are informed of CCTV use during induction and must acknowledge this policy. Any significant changes to camera placement or use are consulted on in advance.

9.2 Complaints: If you believe CCTV is being used inappropriately, please refer to the **Whistleblowing Policy** or the **Complaints Policy**. You also have the right to lodge a complaint with the **Information Commissioner's Office (ICO)**.

9.3 Contact: Data Controller: Innsworth Preschool Peter Scheidel **Contact:**
data@innsworthpreschool.co.uk

