



Closed-Circuit Television (CCTV) Policy 2026/28

Effective Date: 1st September 2026

Last Reviewed: June 2026

Reviewed By: The Open Door Academy Team

Next Review Date: July 2028

Version: 2

CCTV Policy 2025/26



Contents

Introduction.....	3
Purpose of This Policy	3
System Overview.....	3
Legal Basis & Data Protection	3
Location of Cameras	4
Access & Authorised Personnel.....	4
Storage, Retention & Security	4
Subject Access Requests (SARs).....	4
Breaches & Complaints	5
Review.....	5

CCTV Policy 2025/26



Introduction

The Open Door Academy structured CCTV policy is aligned with UK GDPR, ICO CCTV Code of Practice, and common academy-trust standards.

Purpose of This Policy

The purpose of this CCTV Policy is to regulate the management, operation, and use of Closed-Circuit Television (CCTV) at The Open Door Academy. The system is installed to:

- Protect students, staff, visitors, and property
- Reduce crime, anti-social behaviour, vandalism, and trespassing
- Support safeguarding and behaviour management
- Assist police and external agencies when required
- Ensure a safe and secure learning environment

This policy ensures compliance with UK GDPR, the Data Protection Act 2018, and guidance from the Information Commissioner's Office (ICO).

Scope This policy applies to:

- All CCTV cameras and recording equipment owned or operated by The Open Door Academy
- All staff authorised to access CCTV footage
- All individuals on academy premises whose images may be captured
- All data processed, stored, or transmitted via the CCTV system

System Overview

The Open Door Academy operates a CCTV system consisting of:

- Fixed-position doorbell camera covering entrance
- Secure, password-protected recording equipment
- The system is owned and managed by The Open Door Academy.

Legal Basis & Data Protection

CCTV processing is justified under legitimate interests (Article 6(1)(f) UK GDPR) for:

- Preventing crime
- Safeguarding students
- Ensuring site security
- Supporting investigations into incidents

A Data Protection Impact Assessment (DPIA) has been completed and will be reviewed annually or when new cameras/technology are added. **Purposes**

of CCTV Use CCTV is used for:

CCTV Policy 2025/26



- Protecting academy buildings and assets
- Reducing crime, theft, vandalism, and anti-social behaviour
- Assisting police investigations

CCTV is not used for covert monitoring unless authorised under exceptional circumstances (e.g., serious crime) and only with approval from the Directors.

Location of Cameras

Cameras are positioned to capture only areas relevant to the purposes above. They will not be placed in areas where there is a heightened expectation of privacy (e.g., inside toilets).

Signage is displayed prominently across the site to ensure transparency.

Access & Authorised Personnel

Access to live feeds and recorded footage is strictly limited to:

- Directors
- Head of Academy
- Designated Safeguarding Lead (DSL) All access is logged and monitored.

Storage, Retention & Security

Footage is stored securely on encrypted, password-protected systems.

Standard retention period: 30 days, unless required for an investigation.

Footage relating to incidents may be retained longer in line with legal requirements.

Data is automatically overwritten after the retention period.

Sharing & Disclosure Footage may be shared with:

- Police
- Local Authority safeguarding teams
- Legal representatives
- Insurers (where relevant)

Footage will not be shared with parents, students, or third parties unless legally required.

All disclosures are recorded in an Access Log.

Subject Access Requests (SARs)

Individuals may request access to footage in which they appear. Requests must:

- Be made in writing
- Provide sufficient detail to identify the time and location

CCTV Policy 2025/26



- Be assessed for third-party privacy before release
- Footage may be redacted or refused if it compromises others' privacy or ongoing investigations.

Breaches & Complaints

Any breach of this policy or misuse of CCTV will be treated as a disciplinary matter.

Complaints should be directed to:

- Directors

Review

This policy will be reviewed bi-annually by:

- Directors
- Data Protection Officer

The review will consider:

- System effectiveness
- Changes in legislation
- Safeguarding requirements
- Feedback from stakeholders