CCTV DPIA (Data Protection Impact Assessment) 2025/26

Effective Date: 1st September 2025

Last Reviewed: September 2025

Reviewed By: The Open Door Academy Team

Next Review Date: July 2026

Version: 1

CCTV DPIA
(Data Protection Impact Assessment)
2025/26

Contents

CCTV DPIA
(Data Protection Impact Assessment)
2025/26

Introduction
The Open Door Academy is structured exactly as required by the ICO and suitable for Directors, auditors, and Head of Academy.

CCTV Data Protection Impact Assessment (DPIA)

- Date Completed: September 2025
- Review Cycle: Annual or when system changes occur
- Completed by: Head of Academy
- Approved by: IT Director

Project Overview
- **Name of processing activity:** CCTV Monitoring System
- **Purpose:** To ensure the safety and security of students, staff, visitors, and academy property; to prevent and detect crime; to support safeguarding and behaviour management; and to assist investigations.
- **System description:** The academy operates fixed-position Doorbell camera on external areas. Footage is recorded on secure, encrypted systems with restricted access.

Why a DPIA Is Required:
A DPIA is required because CCTV involves:
- Systematic monitoring of publicly accessible areas
- Large-scale processing of identifiable individuals
- Potential safeguarding implications
- Processing of vulnerable groups (children)

This aligns with UK GDPR Article 35(3)(c) and ICO guidance.

Nature, Scope, Context, and Purposes of Processing
3.1 Nature
- Continuous video recording
- Limited live monitoring by authorised staff
- Storage of footage for up to 30 days
- Retrieval of footage for incident investigation
- Secure sharing with police or safeguarding agencies when necessary

3.2 Scope

- All individuals entering academy premises
- Approx. 50 individuals captured daily

3.3 Context

- The academy supports vulnerable students, including those with SEND and safeguarding needs
- CCTV is part of wider safeguarding and behaviour systems
- The academy must comply with UK GDPR, DPA 2018, and ICO CCTV Code of Practice

3.4 Purposes

- Crime prevention and detection
- Safeguarding and welfare monitoring
- Behaviour management
- Protection of academy property
- Supporting investigations

Consultation

Stakeholders consulted:

- Senior Leadership Team
- Designated Safeguarding Lead
- Directors
- Staff representatives

Summary: Stakeholders agreed CCTV is necessary for safeguarding and security. Concerns about privacy were addressed through strict access controls, signage, and limited retention.

Assessment of Necessity & Proportionality

5.1 Lawful Basis

Article 6(1)(f) – Legitimate Interests The academy has a legitimate interest in protecting students, staff, and property.

5.2 Data Minimisation

- Cameras positioned only where necessary
- No recording in private areas
- Access restricted to authorised staff
- Footage retained only for 30 days

5.3 Transparency

- Clear signage displayed
- CCTV policy published on academy website
- DPIA available on request

5.4 Rights of Individuals

- Subject Access Requests permitted
- Redaction applied to protect third parties
- Requests may be refused if they compromise safeguarding or investigations

Risks to Individuals:

Risk	Impact	Likelihood	Overall Risk
Unauthorised access to footage	High	Low	Medium
Excessive monitoring	Medium	Low	Low
Misuse of footage	High	Low	Medium
Data breach (loss or theft)	High	Low	Medium
Inadequate signage / lack of transparency	Medium	Low	Low
Harm to vulnerable students if footage is misused	High	Low	Medium

Measures to Reduce or Eliminate Risks

Risk	Mitigation Measures	Residual Risk
Unauthorised access	Password-protected system; access logs; restricted staff access	Low
Excessive monitoring	Cameras placed only in necessary areas; no covert monitoring	Low
Misuse of footage	Staff training; disciplinary policy; strict sharing rules	Low
Data breach	Encrypted storage; secure servers; automatic overwrite	Low
Lack of transparency	Clear signage; published CCTV policy	Low
Safeguarding concerns	DSL oversight; secure sharing protocols	Low

CCTV DPIA
(Data Protection Impact Assessment)
2025/26

Data Retention

- Standard retention: 30 days
- Extended retention only for active investigations
- Automatic deletion after retention period
- Retention schedule reviewed annually

Data Sharing

Footage may be shared with:

- Police
- Local Authority safeguarding teams
- Legal representatives
- Insurers (where relevant)
- All sharing is logged and authorised by the Directors or DSL.

System Security

- Encrypted storage
- Audit logs
- Regular maintenance and testing
- Annual review by IT Director

Approval & Sign-off

IT Director name:	David Washington	Date:	September 2025
Signature: