



CCTV POLICY

2026-2027

OWNERSHIP:

Everything Education School

AUTHORISED BY:

M Hussain (Headteacher)

EFFECTIVE FROM:

1/9/2026

REVIEW:

1/9/2027

Everything Education School

1234-1238 Coventry Road, Yardley, Birmingham B25 8BZ

CONTENTS

1.0 Purpose and Principles	3
2.0 Legal and Regulatory Framework	3
3.0 Scope	3
4.0 Roles and Responsibilities	3
5.0 Purposes and Lawful Use of CCTV	4
6.0 Camera Locations, Privacy and Signage	4
7.0 Operation, Monitoring and Security	4
8.0 Retention, Review and Deletion	5
9.0 Access, Subject Access Requests and Redaction	5
10.0 Disclosure and Sharing of Footage	5
11.0 Safeguarding, Incidents and Law Enforcement	6
12.0 Data Breaches and Complaints	6
13.0 DPIAs, System Changes and Review	6
14.0 Training, Audit and Policy Review	6
Appendix 1 - CCTV Access / Disclosure Log	7
Appendix 2 - CCTV Compliance Checklist	7

1.0 PURPOSE AND PRINCIPLES

Everything Education School uses closed-circuit television (CCTV) as a proportionate security and safeguarding measure. The system supports the safety of pupils, staff, parents/carers, visitors and the school premises while respecting the privacy and data-protection rights of individuals.

CCTV will be operated lawfully, fairly, transparently and only for specified purposes. It will not be used simply because technology makes monitoring possible, and the school will keep its use under regular review to ensure that it remains necessary and proportionate.

2.0 LEGAL AND REGULATORY FRAMEWORK

This policy is informed by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and relevant amendments made by the Data (Use and Access) Act 2025. It also takes account of Information Commissioner's Office (ICO) guidance on video surveillance, including CCTV, and the wider principles of the Protection of Freedoms Act 2012 and the Surveillance Camera Code where relevant.

Images of identifiable people are personal data. Where footage reveals or is used to infer particularly sensitive information, additional data-protection requirements may apply. The school will identify and document an appropriate lawful basis for its CCTV processing and will apply data protection by design and default.

3.0 SCOPE

This policy applies to fixed CCTV cameras operated by or on behalf of Everything Education School on the school premises and to the viewing, recording, storage, retrieval, copying, disclosure and deletion of CCTV footage. It applies to staff, contractors and any other person authorised to access the system.

The policy does not authorise covert surveillance, body-worn video, facial recognition, audio recording or other enhanced surveillance technologies. Any proposal to introduce such technology must be separately assessed, including a data protection impact assessment where required, and approved before use.

4.0 ROLES AND RESPONSIBILITIES

Everything Education School is the data controller for CCTV footage that it determines the purposes and means of processing. The Headteacher has overall responsibility for ensuring that the CCTV system is operated in accordance with this policy and the school's data-protection arrangements.

- The Headteacher / data-protection lead will oversee lawful use, access controls, retention, disclosures, requests for footage, reviews and staff awareness.
- Only specifically authorised staff may access live or recorded footage. Access must be limited to what is necessary for their role.
- Any contractor maintaining the CCTV system must be subject to appropriate confidentiality, security and data-processing requirements.

5.0 PURPOSES AND LAWFUL USE OF CCTV

The school may use CCTV for the following specified purposes:

- helping to provide a safe and secure environment for pupils, staff, parents/carers, visitors and contractors;
- preventing, deterring and assisting with the detection of crime, theft, vandalism, unauthorised access and damage to school property;
- supporting the investigation of accidents, incidents, safeguarding concerns, serious behaviour incidents or security events where footage is relevant;
- providing evidence to authorised agencies, including the police, where disclosure is lawful and necessary; and
- supporting the management of site safety and security.

CCTV will not be used for routine staff performance monitoring, general surveillance of pupils for educational assessment, publicity, social media or any incompatible purpose. Any exceptional use must be separately justified, lawful and documented.

6.0 CAMERA LOCATIONS, PRIVACY AND SIGNAGE

Cameras may be positioned internally and externally where there is a justified security or safeguarding need. Camera fields of view will be configured to minimise unnecessary capture of neighbouring premises, public areas or other spaces outside the school's legitimate area of concern.

- Cameras will not be installed in toilets, changing areas or other locations where individuals have a heightened expectation of privacy.
- No cameras will be deliberately hidden from view for routine school surveillance.
- Clear and prominent signs will inform pupils, staff, visitors and members of the public that CCTV is in operation and identify the school as the operator or provide a route to further privacy information.
- Where a camera location materially changes, the school will reassess necessity, proportionality and privacy impact before continued use.

7.0 OPERATION, MONITORING AND SECURITY

The CCTV system may record continuously, including outside school hours, where this is necessary for security. Live viewing will be limited to authorised purposes and recorded footage will only be accessed when there is a legitimate reason to do so.

- Recording equipment and administrator accounts will be secured against unauthorised access, alteration, deletion or disclosure.
- Remote access, where enabled, will use appropriate authentication and security controls and will be restricted to authorised users.
- Footage will not be copied to personal devices, personal cloud storage or unauthorised removable media.
- Where footage is exported for an authorised purpose, it will be stored securely, access-controlled and deleted when no longer required.

8.0 RETENTION, REVIEW AND DELETION

Routine CCTV footage will normally be retained for up to 31 days and then automatically overwritten or securely deleted, unless a shorter period is sufficient for the purpose of the system. The school will periodically review whether the retention period remains necessary and proportionate.

Footage may be retained for longer where it is required for an active safeguarding matter, complaint, accident investigation, disciplinary process, insurance issue, legal claim, police enquiry or other legitimate purpose. Any extended retention must be limited to the relevant footage and reviewed so that it is deleted when no longer required.

9.0 ACCESS, SUBJECT ACCESS REQUESTS AND REDACTION

Individuals have data-protection rights in relation to CCTV images in which they can be identified. A request for personal data captured by CCTV will be handled under the school's data-protection procedures and applicable statutory timescales. Requests do not have to use a particular form, although the school may ask for information such as the date, approximate time, location and a description to help locate the footage.

Before releasing footage, the school will consider the rights and privacy of other people shown. It may use redaction, masking, still images, supervised viewing or another appropriate method where necessary. The consent of every person appearing in the footage is not automatically required; disclosure decisions will be made in accordance with data-protection law and any applicable exemptions.

A request may be refused or restricted where an applicable legal exemption or restriction applies. Where appropriate, the requester will be informed of the decision, the reasons and their right to complain.

10.0 DISCLOSURE AND SHARING OF FOOTAGE

CCTV footage will not be routinely shared. Disclosure will be limited to what is necessary, proportionate and lawful for the purpose concerned. Possible recipients may include:

- the police or other law-enforcement bodies in connection with prevention or detection of crime, safeguarding or an investigation;
- children's social care, emergency services or other safeguarding partners where disclosure is necessary to protect a child or another person;
- insurers, legal advisers, courts, tribunals or other bodies where required for a legal claim, statutory function or legal obligation; and
- an individual exercising their data-protection rights, subject to the rights of others and any applicable restrictions.

Where footage is disclosed, the school will keep an appropriate record of the reason, recipient, date, authorising person and material disclosed. Secure transfer methods will be used.

11.0 SAFEGUARDING, INCIDENTS AND LAW ENFORCEMENT

CCTV may support safeguarding and incident investigation, but it does not replace staff supervision, safeguarding practice or professional judgement. If footage indicates that a child may be at risk of harm, the matter will be referred promptly to the Designated Safeguarding Lead and managed under the Safeguarding and Child Protection Policy.

Where police or another statutory agency requests footage, the school will verify the request where appropriate and consider the lawful basis for disclosure. Urgent disclosure may take place where necessary to protect life, prevent serious harm or support a lawful investigation.

12.0 DATA BREACHES AND COMPLAINTS

Loss, unauthorised access, inappropriate viewing, accidental disclosure, cyber compromise or other misuse of CCTV footage must be reported immediately to the Headteacher / data-protection lead and managed under the school's personal data breach procedure. The school will assess whether notification to the ICO and/or affected individuals is required.

Concerns about the operation of CCTV should be raised with the Headteacher in the first instance. Data-protection complaints will be handled under the school's data-protection complaints process. Individuals may also have the right to complain to the Information Commissioner's Office.

13.0 DPIAs, SYSTEM CHANGES AND REVIEW

The school will consider privacy and data-protection risks before installing new cameras or materially changing the purpose, coverage or capability of an existing system. A data protection impact assessment (DPIA) will be completed where the proposed processing is likely to result in a high risk to individuals' rights and freedoms or where otherwise required by law or ICO guidance.

The school will not enable facial recognition, biometric identification, systematic audio recording, covert monitoring or other materially more intrusive functions without a separate lawful assessment, appropriate approval and any required consultation or DPIA.

14.0 TRAINING, AUDIT AND POLICY REVIEW

Staff authorised to access CCTV will be made aware of confidentiality, security, acceptable use, disclosure and data-protection requirements. The school will periodically review camera locations, signage, access permissions, retention settings, disclosure records and system security.

This policy will be reviewed at least annually and sooner where there is a significant change to the CCTV system, relevant legislation, ICO guidance, school premises or safeguarding arrangements.

RELATED POLICIES

Safeguarding and Child Protection Policy
Data Management / Data Protection Policy
Complaints Procedure
Staff Code of Conduct
Behaviour Policy
Premises / Health and Safety arrangements

APPENDIX 1 - CCTV ACCESS / DISCLOSURE LOG

The following information should be recorded whenever recorded CCTV footage is reviewed, exported or disclosed for a specific incident or request.

Date / time of access	
Person accessing footage	
Reason / incident reference	
Date / time range viewed	
Camera(s) / location	
Action taken / footage exported	
Recipient (if disclosed)	
Lawful reason / authority for disclosure	
Method of secure transfer	
Date retained footage due for deletion	
Authorisation / notes	

APPENDIX 2 - CCTV COMPLIANCE CHECKLIST

- ☐ The purposes for CCTV use are documented and remain necessary and proportionate.
- ☐ Camera locations avoid toilets, changing areas and other high-privacy spaces.
- ☐ Camera fields of view are limited to what is necessary.
- ☐ Prominent CCTV signage is in place and privacy information is available.
- ☐ Access to live and recorded footage is restricted to authorised users.
- ☐ Retention is set appropriately and routine footage is deleted/overwritten when no longer needed.
- ☐ Exports and disclosures are logged and transferred securely.
- ☐ Subject access requests can be located, reviewed and redacted where required.
- ☐ A DPIA is completed where high-risk surveillance processing is proposed.
- ☐ Camera locations, permissions, security and retention are reviewed periodically.