

GATEWAY ACADEMY



Gateway Academy CCTV Policy

Approved by:	Lisa Breslin and Claire Cleary
--------------	--------------------------------

Last reviewed on:	October 2026
-------------------	--------------

Next review due by:	October 2027
---------------------	--------------

PURPOSE, SCOPE AND PRINCIPLES

Gateway Academy uses closed-circuit television (CCTV) as a proportionate measure to help safeguard pupils, staff and visitors; manage incidents and emergencies; prevent and detect crime; and protect buildings, facilities and property. This policy applies to everyone whose identifiable images may be recorded, including pupils, parents and carers, employees, contractors, visitors and individuals immediately outside the premises. The system is not guaranteed to capture every incident and does not replace supervision, safer recruitment, safeguarding controls or effective site security.

The Academy will process CCTV personal data lawfully, fairly, transparently and securely; collect no more than necessary; limit access and retention; and demonstrate accountability. This policy operates alongside the Data Protection Policy, Privacy Notices, Record of Processing Activities (RoPA), DPIA, records retention schedule, Subject Access Request procedure, safeguarding and child protection policy, staff conduct procedures and information security policy.

LEGAL FRAMEWORK AND LAWFUL BASIS

Relevant law and guidance includes the UK GDPR and Data Protection Act 2018 (as amended, including by the Data (Use and Access) Act 2025), Human Rights Act 1998, Freedom of Information Act 2000, Protection of Freedoms Act 2012, relevant surveillance camera code principles, ICO video surveillance guidance and the Department for Education's Data protection in schools guidance (including the October 2026 DUAA checklist). The application of the Regulation of Investigatory Powers Act 2000 to any proposed investigatory activity must be assessed specifically; it must not be assumed that school authorisation confers statutory investigatory powers.

For CCTV necessary to perform the Academy's educational, safeguarding and related public functions, the anticipated lawful basis is UK GDPR Article 6(1)(e) (public task), supported by the Academy's underlying legal responsibilities. The Academy will record the purpose, relevant statutory functions and necessity assessment in its DPIA/RoPA. Article 6(1)(f) (legitimate interests) must not be asserted merely because footage includes the public highway; it may only be relied upon for genuinely separate activities where available, with a documented legitimate interests assessment. Consent is not relied upon for routine CCTV. Any footage revealing special category or criminal offence information must be subject to the further applicable UK GDPR/DPA safeguards when it is processed for such purposes.

GOVERNANCE AND ACCOUNTABILITY

The Academy, acting through its trust, is the data controller and is accountable for CCTV decisions; the DPO provides independent advice and monitors compliance.

The CoHeadteachers are responsible for operational implementation, approval of exceptional access and escalation of concerns; the Board of Trustees oversees policy approval and assurance under the Academy's Scheme of Delegation.

The designated CCTV system administrator [confirm named post] maintains the restricted camera register, permissions register, audit logs, system checks and maintenance records.

The Designated Safeguarding Lead (DSL) advises on risks and urgent safeguarding use; safeguarding decisions remain subject to lawful and proportionate handling.

The DPO must be consulted before significant changes and may advise on DPIAs and rights requests; legal accountability does not transfer to the DPO.

CAMERAS, PLACEMENT AND SYSTEM SPECIFICATION

There are 21 internal and external cameras operating day and night. Every camera has a documented purpose, location, field of view, recording hours and any privacy masks. Coverage should be minimised to necessary areas. Footage of roads, pavements, neighbouring flats, private entrances or windows will be avoided or masked unless justified by a documented necessity and proportionality assessment.

Cameras must not be placed in toilets, changing facilities or similarly private spaces. The Academy does not routinely record in classrooms or private offices; any exceptional proposal requires a fresh necessity assessment, consultation, DPIA, safeguarding review and appropriate governance approval before installation. Cameras around Nursery/Reception outdoor spaces and other areas used by younger or vulnerable children will have a specific risk assessment undertaken. Camera location details that would compromise security may be kept in a restricted annex.

Audio, biometrics and additional functions

The Academy will not routinely record conversations or sound and will not deploy facial recognition, biometric identification, automated profiling or automatic number-plate recognition as part of ordinary CCTV. These capabilities must be disabled by default where present. A proposal to activate any such technology must not proceed until the Academy has conducted a separate assessment of legal basis, necessity, proportionality, safeguarding impact, DPIA and appropriate consultation and approval. System updates must be checked to ensure disabled capabilities remain disabled.

DEFINED PERMITTED PURPOSES AND INAPPROPRIATE USES

- Protect the welfare and physical safety of pupils, staff and visitors, including during entry, exit and emergencies.
- Protect the site, buildings, equipment and property from damage, unauthorised access, theft and vandalism.
- Prevent, identify and investigate security incidents, accidents and suspected criminal behaviour.
- Assist safeguarding enquiries and serious incident investigations when necessary and proportionate.
- Provide relevant evidence to police, children's social care, courts, insurers or others where a lawful disclosure is justified.

CCTV will not be used for routine employee performance assessment, monitoring teaching quality or productivity, enforcing ordinary classroom discipline, marketing, or publication on social media. Footage may exceptionally support investigation of serious staff misconduct where use is compatible with the original purpose or separately justified, fair, necessary, proportionate and documented; relevant employment procedures must also be followed.

TRANSPARENCY, CONSULTATION AND SIGNAGE

The Academy will place legible CCTV notices before or at monitored entrances and in other appropriate locations, stating that CCTV operates, its main purposes, the controller's identity and a clear route to the full privacy notice and contact details. The dedicated CCTV privacy notice will be published on the Academy website and available in accessible formats. Where changes materially alter surveillance, the Academy will consult pupils (in an age-appropriate way), parents and carers, staff and the DPO, and consider less intrusive alternatives before implementation.

ACCESS, PERMISSIONS AND AUDIT TRAILS

Access to CCTV footage is restricted to authorised staff who have received appropriate training and have a clear, work-related reason for accessing it.

The Academy maintains an up-to-date record of authorised users and their access permissions. Permissions are reviewed when staff responsibilities change and removed promptly when no longer required. The Academy's CCTV Privacy Notice identifies the categories of staff who may access footage.

Access permissions are as follows:

- **Live CCTV footage:** Access is restricted to authorised staff responsible for site safety and security. Reception staff may view live footage for entrance security purposes where specifically authorised, but this does not automatically permit access to recorded footage.
- **Recorded CCTV footage:** Access to previous recordings is restricted to the CoHeadteachers and other specifically authorised and trained staff.
- **Downloading and sharing footage:** Only designated senior staff may authorise and carry out the downloading or disclosure of footage. Where urgent safeguarding or security circumstances require an exception, the reasons and actions taken must be recorded and subsequently reviewed.
- **IT support and contractors:** Access is limited to what is necessary to maintain or repair the system. Any access to recorded images must be justified and logged. External contractors must comply with relevant confidentiality, data protection and security requirements.

Security arrangements

The Academy will ensure that:

- Each authorised user has an individual account and secure login details.
- Access permissions are limited to what each person's role requires.
- CCTV monitors and recording equipment are protected from unauthorised viewing or access.
- Footage is not recorded, downloaded, stored or shared using personal devices or personal messaging applications.
- Access to CCTV footage is monitored and recorded appropriately.

Access and audit records

Whenever recorded footage is reviewed, downloaded or disclosed, the Academy will maintain a record of:

- The date and time of access.
- The name of the person accessing the footage.
- The person requesting access, where applicable.
- The reason for accessing the footage.
- The cameras involved and the relevant recording period.
- Who authorised access or disclosure.
- Any actions taken, including whether footage was downloaded, shared or retained.

Any exceptional or unauthorised access will be investigated and documented in accordance with the Academy's data protection and information security procedures.

Access logs will be reviewed periodically, with any concerns investigated promptly. The list of authorised users and their permissions will be formally reviewed at least annually, and sooner where staffing or responsibilities change.

STORAGE, CYBERSECURITY AND RETENTION

There is local digital recording in a locked cabinet in Reception and uses encrypted school systems. Footage is protected by secure devices, patched software, restricted accounts and robust backup/restore and incident-response arrangements as appropriate.

The proposed routine footage retention period is 30 calendar days, after which footage is automatically overwritten/deleted. Footage needed for an identified safeguarding, police, insurance, complaint, disciplinary or legal matter may be securely preserved before overwrite only for as long as necessary, with a recorded reason, owner, review date and secure deletion date. Exports are subject to the same restrictions and cannot remain indefinitely in email, shared drives or portable media.

SUBJECT ACCESS AND OTHER DATA PROTECTION RIGHTS

Individuals may request their personal data in CCTV footage verbally or in writing; the Academy must recognise and promptly forward requests even if they are not addressed to the DPO. Requests should ideally include the incident date/time, location and enough information to locate the footage, but must not be rejected solely for not using a prescribed form. Where appropriate, identity or parental responsibility/authority may be checked. Access to a child's footage depends on the child's rights, competence, best interests and applicable representation, not an automatic entitlement for any adult.

Requests will normally be answered without undue delay and within one calendar month, subject to applicable lawful extensions or pauses for necessary clarification under the amended law. Searches must be reasonable and proportionate. When relevant footage is held, the Academy will consider privacy-preserving disclosure, redaction of other identifiable individuals, viewing arrangements or a lawful exemption. It will preserve potentially responsive footage on receipt of a request where necessary to prevent routine deletion during handling. An inability to identify or retrieve footage, or lawful deletion before receipt of a request, must be explained accurately.

Other applicable rights include rectification, erasure, restriction and objection; their application to fixed factual recordings and public-task processing depends on the circumstances. Complaints and requests must be recorded and decisions explained.

DISCLOSURE AND SAFEGUARDING REQUESTS

CCTV may be disclosed only where a documented legal basis and an appropriate necessity/proportionality assessment support it, or where there is a binding legal obligation. The Academy may receive requests from police, children's social care, statutory safeguarding agencies, courts, insurers, legal advisers and individuals acting with valid authority. A police request is not automatically a legal command; the Academy will obtain sufficient information to assess the scope and basis of voluntary disclosure. Court orders will be reviewed for precise requirements. Information must be minimised, securely transferred and appropriately redacted where necessary.

Where there is an urgent risk of significant harm to a child or another person, relevant information may be shared promptly where lawful and necessary; staff must not delay protective action solely to obtain ordinary administrative approval. The DSL and CoHeadteachers should be informed as soon as practicable, and the reason, material shared, recipient and authorisation must be recorded. The Academy will preserve an evidentially reliable copy, noting chain of custody and any redactions.

COVERT OR TARGETED SURVEILLANCE

Covert surveillance is not a routine Academy activity. Any exceptional proposal requires contemporaneous legal advice on applicable surveillance/investigatory law, a specific DPIA, evidence that overt/less intrusive measures are inadequate, consideration of children's rights, a tightly specified target/purpose and duration, and written authorisation at appropriate senior governance level. DPO advice will be documented. The activity must stop when its justification ends; the Academy will record and review deletion and any resultant disclosure.

CONTRACTORS, TRANSFERS AND DATA BREACHES

Before permitting any CCTV service provider to access personal data, the Academy must establish controller/processor roles, enter required Article 28 terms where applicable and assess security, sub-processors, remote access and international transfers. Any suspected loss, inappropriate viewing, unauthorised disclosure or cyber incident will be reported immediately through the Academy's data-breach procedure; the DPO will advise on assessment and whether notification to the ICO within 72 hours of awareness or communication to affected individuals is required.

COMPLAINTS, TRAINING, MONITORING AND REVIEW

Individuals may raise privacy concerns with Gateway Academy through its normal contact channels or DPO, in writing, by email or verbally. Data protection complaints must be acknowledged within 30 days, investigated without undue delay, logged, and the complainant informed of progress and outcome. Individuals may complain to the ICO, with details in the privacy notice. Authorised staff will receive induction and periodic refresher training. The controller will review the DPIA, retention, access logs, camera masking, supplier contracts, signage and policy at least annually and following material changes, incidents or updated guidance.

OFFICIAL GUIDANCE CONSULTED

DfE: <https://www.gov.uk/guidance/data-protection-in-schools/taking-and-using-photos-and-videos-and-using-cctv-in-schools>

DfE (14 October 2026): <https://www.gov.uk/guidance/data-protection-in-schools/data-use-and-access-act-2025-duaa-compliance-checklist-for-schools>

ICO: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/>

Appendix 1 – CCTV Signage

It is a requirement of the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the school
- The contact telephone number or address for enquiries



Appendix 2 - Checklist

This CCTV system and the images produced by it are controlled by the Headteacher who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 2018).

Gateway Academy has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			

There is a named individual who is responsible for the operation of the system.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Staff and members of the Academy community will be consulted about the proposal to install CCTV equipment.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, and only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The Academy knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix 3 – Incident Log

Incident Occurrence Log

Date:				
Start Time	Area	Occurrence /Event	Camera nos.	Signature (Data Controller)

Incident Occurrence Log

Date:				
Start Time	Area	Occurrence /Event	Camera nos.	Signature (Data Controller)

Incident Occurrence Log

Date:				
Start Time	Area	Occurrence /Event	Camera nos.	Signature (Data Controller)

Incident Occurrence Log

Date:				
Start Time	Area	Occurrence /Event	Camera nos.	Signature (Data Controller)

Appendix 4 – Police Log

CCTV: VIDEO REVIEW BY POLICE & STILLS LOG (if any printed)

Date.....Time.....

Incident Date & Time From..... Date & Time To.....

Incident:

Video Details:

Camera(s)..... Date.....Time.....

Camera(s)..... Date..... Time.....

Camera(s)..... Date..... Time.....

Officer's Name / Number..... Telephone No.....

Signature.....Date.....

Result.....

STILLS PRINTED? (If yes, then complete below)

1.
Still ID.....Camera.....Date.....Time.....

2.
Still ID.....Camera.....Date.....Time.....

3.
Still ID.....Camera.....Date.....Time.....

4.
Still ID.....Camera.....Date.....Time.....

5.
Still ID.....Camera.....Date.....Time.....

Operator

Name.....

Operator: Signature.....