



CLOSED CIRCUIT TELEVISION (CCTV) POLICY

Approved By: Trust Board
Approval Date: October 2026

CONTENTS

1. Purpose and Scope.....	3
2. Principles Governing the Use of CCTV.....	3
3. Legislation and Guidance	3
4. Definitions	4
5. Roles and responsibilities.....	5
6. Training, competency and authorisation	7
7. Purposes and Permitted Use of CCTV	7
8. Installation and Location of Cameras.....	9
9. Access to CCTV	10
10. Live CCTV Monitoring.....	11
11. Storage and Retention of CCTV	11
12. Audio Recording.....	12
13. Subject Access Requests (SAR)	13
14. Complaints	13
Appendix One: Template CCTV Recording Log	14
Appendix Two Access Levels.....	15

1. PURPOSE AND SCOPE

The Girls' Learning Trust ("the Trust") uses CCTV and other authorised video-surveillance systems as a proportionate tool to support the safe, orderly and effective operation of its schools. CCTV can provide important information to support safeguarding, behaviour management, health and safety, site security, incident response and the investigation of events occurring on school premises.

The Trust recognises that CCTV involves the processing of personal data and can affect the privacy of students, staff and visitors. CCTV will therefore only be used for defined and legitimate purposes and in a manner which is lawful, necessary, proportionate and transparent.

This policy applies both where CCTV images are recorded and retained and where cameras provide a live feed which is viewed but not recorded.

2. PRINCIPLES GOVERNING THE USE OF CCTV

CCTV must be used in a manner which respects the privacy and rights of students, staff, visitors and others using Trust premises. Its use must be:

- Lawful, with an appropriate legal basis for the processing of personal data.
- Necessary, so that surveillance is used only where there is a genuine and defined purpose.
- Proportionate, with the nature and extent of surveillance appropriate to the issue or risk being addressed.
- Transparent, so that individuals are appropriately informed that CCTV is in operation and how it may be used, except where covert surveillance has been specifically authorised.
- Secure, with access to live feeds and recorded footage restricted to authorised staff and appropriate safeguards in place.
- Purpose-limited, so that CCTV is used only for legitimate school or Trust purposes.
- Accountable, with clear arrangements for authorisation, operation, access and oversight.

CCTV is a source of information which supports professional judgement and established school procedures. Footage or live observations may form part of the evidence considered by the school or Trust but need not provide a complete or conclusive record of an incident. Decisions may therefore be reached on the basis of the evidence as a whole, including where CCTV footage is unavailable or inconclusive.

CCTV will normally be operated openly. In exceptional circumstances, the Trust may authorise covert surveillance where there is a specific and compelling reason, the surveillance is lawful, necessary and proportionate, and less intrusive measures would not reasonably achieve the intended purpose. Any covert surveillance must be appropriately authorised, limited in scope and duration, and kept under review. The Data Protection Officer will be consulted where appropriate.

Camera locations, functionality and access arrangements will be reviewed annually to ensure that their continued use remains appropriate. These principles apply to both recorded CCTV and live feeds which are viewed without being recorded

3. LEGISLATION AND GUIDANCE

This policy is informed by, and should be applied consistently with, the following legislation:

- UK General Data Protection Regulation (UK GDPR): governing the lawful, fair and transparent processing of personal data, including images and other information captured through CCTV and video-surveillance systems.
- Data Protection Act 2018 (DPA 2018): supplementing the UK GDPR and providing the wider statutory framework for the processing, protection and disclosure of personal data.
- Data (Use and Access) Act 2025: which amended aspects of the UK GDPR and Data Protection Act 2018.
- Protection of Freedoms Act 2012: providing the statutory framework relating to the appropriate use of surveillance camera systems in public places.
- Human Rights Act 1998: particularly Article 8 of the European Convention on Human Rights, concerning respect for private and family life.
- Equality Act 2010: requiring the Trust to ensure that the operation and use of CCTV does not result in unlawful discrimination.

The policy takes account of current Information Commissioner's Office (ICO) guidance on video surveillance, including CCTV, and the use of monitoring within organisations.

The policy also takes account of Department for Education guidance on data protection in schools, including the use of photographs, video and CCTV.

Where relevant, the Trust will also have regard to the principles contained within the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012.

This policy should be read in conjunction with other relevant Trust and school policies, including:

- Data Protection and Freedom of Information Policy.
- Data and Records Retention Policy.
- Safeguarding and Child Protection Policy.
- School Behaviour Policies.
- IT Policy.
- Staff Code of Conduct.
- Staff Disciplinary Policy.
- Complaints Policy.

4. DEFINITIONS

Accessing CCTV: Any authorised interaction with live or recorded CCTV systems, including monitoring, reviewing, retrieving, preserving, exporting or disclosing CCTV footage.

Viewing CCTV: The act of observing live or recorded CCTV images for an authorised purpose. Viewing does not include exporting, copying, preserving or disclosing footage.

Monitoring CCTV: The ongoing observation of live CCTV feeds in real time.

CCTV Review: The focused examination/viewing of live or recorded footage for a defined and legitimate purpose. This does not include copying, downloading, exporting, sharing or disclosing footage.

Authorised User: A member of staff or other approved individual who has been formally authorised by the Headteacher, CCTV or other designated authority to access CCTV systems and footage in

accordance with this policy and any training and confidentiality requirements.

Exporting CCTV Footage: Creating a copy of recorded CCTV footage from the system into another format, device or storage medium. This includes downloads, screenshots, digital files, USB storage devices, cloud storage locations or other transferable formats.

Disclosure of CCTV Footage: The provision, sharing, release, transfer or permitting access to CCTV footage, or any part of it, to an individual, organisation or authority outside those already authorised to access the CCTV system. Disclosure may include responding to Subject Access Requests, court orders, regulatory requests, safeguarding concerns or request from statutory agencies.

Preserved Footage: CCTV footage that has been identified as relevant to an incident, investigation, complaint, safeguarding matter, legal process, insurance claim, disciplinary process or other legitimate purpose and has been retained beyond the standard retention period to prevent its automatic deletion. Preserved footage shall remain securely stored and accessible only to authorised persons until the relevant matter has been concluded and any retention requirements have been satisfied.

CCTV Access Register: Records individuals authorised to access CCTV systems.

CCTV Recording Log: Records individual instances of substantive access, preservation, export or disclosure of CCTV footage.

5. ROLES AND RESPONSIBILITIES

This policy applies to all staff and volunteers within the Trust, and to external organisations or individuals working on our behalf.

Chief Executive Officer

The Chief Executive Officer has overall accountability for ensuring the policy is adhered to and implemented effectively.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) has specific CCTV responsibilities related to monitoring compliance and providing advice regarding:

- Dealing with subject access requests (SAR) in line with legislation, for any disclosure of CCTV footage held by the Trust.
- Ensuring that all staff at each school within the Trust handle and process CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained and stored in line with legal requirements and the Trust's Records Retention Policy.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects how their data captured in surveillance and CCTV footage will be used by the Trust, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Ensuring each school in the Trust has completed a privacy impact assessment (PIA), and a data protection impact assessment (DPIA), to ensure the use of surveillance and CCTV is justified and monitors the risks of using such systems.

- Ensuring that all relevant staff in the Trust understand their responsibilities as set out in the ICO CCTV Codes of Practice.

Headteacher and CCTV Lead

In each school, the Headteacher is responsible for identifying and appointing a Lead Person (who may be the Headteacher) to lead the management and supervision of CCTV in the school. This individual must be approved by the Trust's Data Protection Officer.

The role and responsibilities of the Lead Person in each school include:

- Ensuring that this policy is followed by all staff, volunteers and students in the school.
- Arranging training for relevant school staff in consultation with the Trust DPO.
- Identifying staff within the school who will be responsible for the operation and viewing of the CCTV system (who will usually include the relevant Premises Manager and Designated Safeguarding Lead).

Chief Infrastructure Officer

The Chief Infrastructure Officer of the Trust is responsible for the overall management of the CCTV infrastructure including:

- The installation, maintenance and upkeep of all hardware.
- The installation and management of all relevant software.
- Ensuring adequate resources are in place within the school to use the CCTV system appropriately.

Premises Manager and local IT Team

The School's Premises Manager and IT Team are jointly responsible for maintaining CCTV cameras and equipment including:

- Escalating school requests for modifications to CCTV to the CIO.
- Ensuring all routine maintenance and servicing is undertaken, including hardware and software updates.
- Identifying and resolving promptly any operational issues and faults.
- Ensuring there is an appropriate connection to the school network.

Summary Table

Chief Executive Officer	Overall accountability for ensuring the policy is adhered to and implemented effectively.
Data Protection Officer	Handling subject access requests (SAR) for CCTV footage. Ensuring CCTV footage is obtained, stored, processed and destroyed according to legal requirements. Informing data subjects about the use of their data. Completing privacy and data protection impact assessments. Ensuring compliance with ICO's CCTV Code of Practice.
Headteacher	Appointing a Lead Person to manage CCTV at the school. Ensuring staff, volunteers and students comply with the policy. Organising relevant staff training in consultation with the DPO.
CCTV Lead	Responsible for managing and supervising CCTV operations.

	Identifying staff authorized to operate and view the CCTV system.
Chief Infrastructure Officer	Managing the CCTV infrastructure. Overseeing the installation, maintenance, and upkeep of CCTV hardware and software.
Premises Manager & IT Team	Jointly responsible for maintaining CCTV cameras and equipment.

6. TRAINING, COMPETENCY AND AUTHORISATION

Training Requirements

No individual shall be permitted to monitor, access, download, export or disclose CCTV footage unless appropriately authorised and trained. This training should cover:

- The principles of UK GDPR and the Data Protection Act 2018 as they relate to CCTV.
- Practical examples of privacy and proportionality considerations relevant to the school setting to demonstrate the balance of reasonable coverage when compared to the risk or issue that is being addressed.
- CCTV access controls and confidentiality.
- Viewing, downloading, storing and sharing footage securely.
- Subject Access Requests and disclosure procedures.
- Incident reporting and data breach requirements.
- The Trust CCTV policy, Records Retention Policy and Data Protection Policy.

Refresher training must be undertaken periodically and whenever there are significant changes to legislation, guidance, systems or Trust procedures. This should be recorded via the established school and Trust systems.

Authorisation Requirements

No member of staff, contractor or external party shall be authorised to access Trust CCTV systems until they have completed the required training and been formally authorised by the Headteacher or CCTV Lead.

The CCTV Access Register is a formal record of authorised users. Access rights will be reviewed at least annually by the DPO and Headteacher and when relevant staff leave, change role or no longer require access.

7. PURPOSES AND PERMITTED USE OF CCTV

CCTV may be used by the Trust and its schools where this is lawful, necessary and proportionate to support the safe, orderly and effective operation of the school. The purposes set out below are not exhaustive; CCTV may also be used for other legitimate school or Trust purposes where these are consistent with the principles set out in this policy.

CCTV, including recorded footage and live feeds, may be used to:

- Support safeguarding and child protection, including identifying students or other individuals involved in an incident, establishing relevant events or movements, responding to concerns and informing decisions about appropriate safeguarding action.
- Support behaviour management, including investigating actual or suspected breaches of school rules or the Behaviour Policy; identifying students involved; establishing the sequence of events;

verifying, supporting or challenging accounts provided by students or others; and informing appropriate pastoral or disciplinary action.

- Investigate bullying, harassment, child-on-child abuse or other inappropriate behaviour, including where CCTV may assist the school in understanding the context, frequency or circumstances of an incident.
- Support pastoral management and student welfare, including locating students, responding to welfare concerns, understanding events affecting a student and supporting appropriate interventions.
- Support the management of complaints, concerns and disputes, including reviewing relevant footage when considering concerns raised by parents, carers, students, staff or other individuals and determining whether accounts of events are consistent with the available evidence.
- Support internal investigations, including safeguarding, behaviour, disciplinary, complaints, health and safety, premises, employment or other investigations undertaken by a school or the Trust.
- Protect the health and safety of students, staff and visitors, including investigating accidents, near misses, unsafe behaviour or other incidents and identifying improvements to working practices or the school environment.
- Support the management of emergencies and significant incidents, including locating individuals, assessing an unfolding situation, managing evacuation or lockdown arrangements and supporting the response of the school or emergency services.
- Maintain the security and orderly operation of school premises, including monitoring entrances, exits, circulation areas, external spaces and other locations where surveillance may reasonably assist the management of the site.
- Protect Trust and personal property, including preventing, detecting and investigating theft, vandalism, criminal damage, trespass or unauthorised access.
- Prevent, deter, detect or investigate criminal or potentially criminal activity, and support the police, emergency services, local authorities or other statutory agencies where appropriate.
- Support the management of visitors, contractors and other persons on school premises, including investigating incidents or concerns relating to their conduct or presence on site.
- Provide evidence in connection with legal, regulatory, insurance or other formal proceedings, where the Trust considers that footage is relevant and its use or disclosure is lawful.

CCTV footage may be reviewed following a reported incident or concern, but the Trust or school may also review footage proactively where information available to it gives reasonable cause to believe that an incident, safeguarding concern, breach of school rules, safety issue or other matter requiring investigation may have occurred.

Where CCTV is considered as part of an investigation or decision-making process, it will normally be considered alongside other available evidence. The fact that an individual's recollection or account differs from what appears on CCTV does not, by itself, determine the outcome of the matter; the school or Trust will consider the evidence as a whole.

A parent, carer, student, member of staff or other individual may ask the school to consider whether relevant CCTV footage exists. However, there is no automatic right to require the school to undertake extensive or speculative searches of CCTV recordings. The school may require sufficient information to identify the likely date, time, location and nature of the incident and will determine what review is reasonable and proportionate in the circumstances.

Similarly, a request that CCTV footage is reviewed as part of a complaint does not create an automatic

right for the complainant to view or receive the footage. Requests for access to, or copies of, CCTV recordings will be considered separately in accordance with the data protection and disclosure provisions of this policy.

CCTV systems operate subject to defined retention arrangements. The Trust cannot guarantee that footage will remain available where an incident or request is raised after the relevant recording has been routinely overwritten or deleted in accordance with those arrangements. Where the Trust or school becomes aware that existing footage is likely to be materially relevant to an ongoing safeguarding matter, investigation, complaint, legal process or other legitimate purpose, it may preserve the relevant footage for as long as reasonably necessary.

The permitted uses within this section apply to both recorded CCTV footage and, where appropriate, information observed through a live CCTV feed.

8. INSTALLATION AND LOCATION OF CAMERAS

The overall placement and coverage of CCTV cameras within each school will be developed and agreed by the Headteacher in consultation with the Chief Infrastructure Officer, subject to approval by the Data Protection Officer. This will include consideration of the purpose of the surveillance, the location and field of view of cameras, privacy implications, proportional use and any particular operational or safeguarding requirements.

Cameras will be positioned so that they capture only images reasonably necessary for the purposes for which they are installed. Where practicable, coverage will be limited to Trust or school premises, including relevant external areas. Where a camera may capture areas beyond the school boundary, this will be limited to what is necessary and proportionate.

Particular care will be taken when considering CCTV in teaching spaces, recognising the greater impact that continuous or routine surveillance may have on staff privacy and professional autonomy. CCTV will not normally be installed in classrooms or other spaces used primarily for teaching. Where there is a specific and justified need for CCTV in a teaching space, this must be supported by an appropriate Data Protection Impact Assessment (DPIA) and approved by the Headteacher and Data Protection Officer, with appropriate consultation undertaken where required. Instances where this might be justified include safeguarding, serious behavioural concerns, or specific risk assessed activities.

This restriction does not apply in the same way to pastoral, welfare, reception, circulation or supervision spaces, where CCTV may appropriately form part of the school's arrangements for safeguarding, behaviour management, student welfare, safety or operational oversight, provided its use remains necessary and proportionate.

CCTV will not normally be installed in areas where individuals have a particularly high expectation of privacy, such as toilets, changing rooms or similar facilities.

Staff will be able to access appropriate information about the location and operation of CCTV cameras within their school, except where disclosure would undermine specifically authorised covert surveillance. Appropriate CCTV signage will be displayed at entrances and within monitored areas.

The Premises and IT teams will work together to ensure that CCTV equipment is appropriately maintained, secure and functioning as intended.

9. ACCESS TO CCTV

Access to CCTV systems, live feeds and recorded footage will be restricted to authorised staff and must be connected to a legitimate professional purpose. The Headteacher, supported by the CCTV Lead, is responsible for determining which staff within the school may access CCTV and the level of access appropriate to their role.

Authorised access may include routine access associated with a member of staff's role, or access granted in response to a particular incident, concern or investigation. Staff may only view CCTV where this is consistent with the purposes and principles set out in this policy.

Different levels of access may be granted according to operational need. This is shown in the CCTV Access Levels and Authorisation table at Appendix Two. Levels of access may include permission to:

- View live CCTV feeds.
- Search and review recorded footage.
- Preserve footage from routine deletion.
- Download or export recordings.
- Administer or configure the CCTV system.

Permission to view CCTV does not automatically include permission to download, export, copy or disclose footage. These functions will be restricted to staff specifically authorised to undertake them. For example, a member of staff may legitimately be permitted to view footage but not export, preserve or disclose it.

Access to recorded footage must be appropriately documented. The school will maintain a record of substantive access to recordings, including the date of access, the individual accessing the footage and the reason for the review. Routine viewing of live feeds does not need to be individually logged where it forms part of an authorised operational arrangement.

Where footage is downloaded, exported or preserved, the record should also identify the footage concerned, the person undertaking the action and the reason for doing so. Extracted footage must be stored securely on an authorised Trust system or device.

Staff must not photograph, screen-record, copy or otherwise reproduce CCTV footage using personal devices or unauthorised systems. CCTV footage must not be shared informally with students, parents, colleagues or other individuals.

Requests from the police, local authorities, insurers, legal representatives, regulators or other third parties must be referred to the Data Protection Officer or another appropriately authorised senior officer. Footage may be disclosed where there is a lawful basis to do so and the disclosure is necessary and proportionate. No CCTV footage may be disclosed externally without approval from the DPO.

Any disclosure of CCTV footage shall be recorded together with the recipient, reason for disclosure, legal basis and the approving officer.

Access rights will be reviewed at least annually and removed or amended where they are no longer required, including when a member of staff changes role or leaves the Trust

10. LIVE CCTV MONITORING

Some CCTV systems may provide a live feed which can be viewed by authorised staff whether or not the images are also being recorded. Live monitoring remains subject to the principles and safeguards set out in this policy.

Live feeds may be used where necessary and proportionate to support the safe, orderly and effective operation of the school. This may include:

- Monitoring entrances, exits, circulation areas, external spaces and other areas requiring supervision.
- Supporting safeguarding, behaviour management and student welfare.
- Locating students or other individuals where there is a legitimate reason to do so.
- Responding to an unfolding incident, concern or emergency.
- Supporting the management of movement, congestion, site access or security.
- Identifying circumstances in which staff intervention or further investigation may be required.

Access to live CCTV feeds will be restricted to staff authorised by the Headteacher or CCTV Lead and should reflect the requirements of their role. Staff must not access or observe live feeds for personal interest, curiosity or any other purpose unrelated to their professional responsibilities.

Live monitoring may be undertaken routinely where this forms part of an authorised operational arrangement, or in response to a particular concern or incident. It is not necessary for there to have been a reported incident before an authorised member of staff may view a live feed where doing so is consistent with the permitted purposes of CCTV set out in this policy.

Screens displaying live CCTV feeds must be positioned or configured so that they cannot be viewed by students, visitors or other unauthorised individuals. Staff must not photograph, record, screen-capture or otherwise reproduce a live feed using a personal or unauthorised device.

Where a member of staff observes an incident through a live feed, that observation may be acted upon and recorded in the same way as any other professional observation. Where the relevant camera does not record footage, the absence of a recording does not affect the ability of the school to rely upon the staff member's observation as part of any subsequent safeguarding, behaviour, complaints or other process.

Live feeds will not normally be made available remotely outside Trust systems unless specifically authorised and appropriate security controls are in place.

11. STORAGE AND RETENTION OF CCTV

Recorded CCTV footage will be retained only for as long as reasonably necessary for the purposes for which it was collected and in accordance with the Trust's Data and Records Retention Policy. Routine recordings may be automatically overwritten or deleted after the applicable retention period.

The Trust does not guarantee that footage will remain available after the normal retention period. Where a school becomes aware, before routine deletion, that particular footage may be relevant to an ongoing safeguarding matter, behaviour or staff investigation, complaint, health and safety incident, insurance claim, legal process, police enquiry or other legitimate purpose, the relevant footage may be preserved for longer.

Footage retained beyond the routine retention period will be kept only for as long as reasonably necessary for the matter concerned and securely deleted when there is no longer a legitimate reason to retain it.

All recorded and preserved footage must be stored securely and protected against accidental loss, alteration, unauthorised access, disclosure or deletion. Where footage is downloaded or exported from the main CCTV system, it must be stored on an authorised Trust system or device and must not be transferred to personal devices, personal cloud storage or other unauthorised locations.

Where footage is retained as evidence, reasonable steps will be taken to preserve its integrity and provenance.

The Chief Infrastructure Officer is responsible for ensuring that appropriate technical arrangements are in place for the security, storage and routine deletion of CCTV recordings. The Headteacher and CCTV Lead are responsible for ensuring that footage retained for a particular school purpose is managed appropriately.

12. AUDIO RECORDING

CCTV systems may include technical functionality capable of recording sound. However, audio recording is significantly more intrusive than the recording of images and will not normally be enabled as part of routine CCTV surveillance.

Where CCTV equipment includes audio capability, this will normally be disabled unless there is a specific and justified reason for its use.

Any proposal to enable audio recording must demonstrate that:

- There is a clearly defined and legitimate purpose.
- Audio recording is necessary and proportionate to achieving that purpose.
- The purpose could not reasonably be achieved through less intrusive means.
- The likely impact on the privacy of students, staff and others has been appropriately considered.

Routine or continuous recording of conversations for general monitoring or staff-management purposes will not be permitted.

Any exceptional use of audio recording must be approved by the Headteacher and Chief Infrastructure Officer, subject to approval by the Data Protection Officer and an appropriate Data Protection Impact Assessment where required. Its use must be limited in scope and duration and kept under review.

Where audio is recorded, it will be subject to the same access, storage, retention, disclosure and data-protection requirements as CCTV images.

13. SUBJECT ACCESS REQUESTS (SAR)

CCTV footage may contain personal data and individuals may have a right to request access to footage in which they can be identified. Any such request will be handled in accordance with the Trust's Data Protection and Freedom of Information Policy, which sets out the Trust's full Subject Access Request procedure, including arrangements for requests made on behalf of children.

Any member of staff who receives a request for CCTV footage must refer it promptly to the Data Protection Officer.

A request for CCTV footage does not automatically entitle the requester to receive an unredacted copy of the recording. The Trust will consider the rights and privacy of other individuals shown in the footage and may redact, obscure, withhold or provide access in another appropriate form where necessary.

The Trust is not required to retain CCTV footage beyond its normal retention period solely because an individual may make a future request. Where footage has already been routinely overwritten or deleted before a request is received, the Trust cannot provide information it no longer holds.

14. COMPLAINTS

General complaints or concerns about the operation or use of CCTV within a school should normally be raised with the Headteacher in the first instance and will be managed in accordance with the Trust's Complaints Policy.

Where a complaint relates specifically to the Trust's compliance with data protection requirements, including the collection, storage, retention, security, access, disclosure or other management of CCTV footage, it will be handled in accordance with the Trust's Data Protection and Freedom of Information Policy and referred to the Data Protection Officer as appropriate.

APPENDIX ONE: TEMPLATE CCTV RECORDING LOG

[illegible]

APPENDIX TWO: ACCESS LEVELS

Access to CCTV systems shall be granted according to operational need and the principle of least privilege. The Trust operates five levels of access and authorisation, as set out below. Authorisation at one level shall not automatically confer access or authorisation at a higher level. Access shall be restricted to specifically authorised staff, with permissions documented and subject to periodic review. The roles identified below are illustrative and do not confer automatic access.

Access Level	Purpose and Permitted Activities	Restrictions and Conditions	Typical Authorised Staff
Level One: Live Monitoring	View live CCTV feeds for site security, safeguarding, health and safety, and emergency response. Staff may observe incidents and report concerns to appropriate colleagues.	No access to recorded footage, exporting, preservation or disclosure.	Headteacher, School CCTV Lead, Premises Manager and other authorised operational staff.
Level Two: Recorded Footage Review	Access and review recorded footage for authorised operational, safeguarding or investigative purposes. Staff may identify footage requiring preservation.	No independent preservation, exporting or disclosure of footage. Access must be limited to the authorised purpose.	All Level One staff, plus School SLT, Designated Safeguarding Lead (DSL) and other authorised senior staff.
Level Three: Preservation, Export and Internal Disclosure	Preserve relevant footage beyond standard retention periods, create secure evidential copies and share footage within the Trust for legitimate safeguarding, disciplinary, operational, legal or other authorised purposes.	Footage must be securely stored and retained only for as long as necessary. All preservation, exports and internal disclosures must be documented, including the purpose, authorising staff member and recipient(s), where applicable. No external disclosure without Level Four authorisation.	Headteacher, DSL, School CCTV Lead and other senior staff specifically authorised by the Trust.
Level Four: External Disclosure Authorisation	Authorise the lawful disclosure of footage outside the Trust, including to the police, local authorities, courts, regulators, insurers and individuals exercising information rights.	Disclosure must be lawful, necessary, proportionate and documented. The Data Protection Officer (DPO) must be consulted where appropriate. Footage must be shared securely and in accordance with applicable data protection requirements.	DPO, CEO and other designated senior staff, acting within their delegated authority.