Grove Learning Trust

Surveillance and Closed Circuit Television (CCTV) Policy

Reviewed centrally
Date: Summer 2026

Contents

Version Control 3
Vision 4
Statement of Intent 4
Principles 4
Legal Framework 5
CCTV and Insurance 5
Definitions 5
Roles and Responsibilities 6
Protocols 8
Security 8
Access 8
Monitoring and Review 10
Appendix 1 – CCTV and Insurance (RPA) 11

Version Control

Version	Date	Status	Author (AU) / Approver (AP)
Draft	May 2025	Completion of first draft	AG (AU)
Draft	June 2025	Feedback from head teacher working party	JW, KS, SC, LC
Final	Summer 2025	Ratified by RAR committee	RAR (AP)

Review

Next Review	Summer 2027

Vision

As one organisation, our vision for Grove Learning Trust is unapologetically bold. We are all about creating remarkable futures. For our children, our people, our places of work, we want the very best. We know that strong connections will enable us to achieve our vision, in a world where purposeful collaboration, based on mutual respect and trust, helps us to achieve more together.

Trust >> Connect >> Collaborate

Our policies underpin our vision and set out clearly our expectations of each other.

Statement of Intent

At Grove Learning Trust, we take our responsibility towards the protection of our estate, and the safety of staff, visitors and children very seriously. To that end, we use surveillance cameras (known as CCTV: closed-circuit television) to monitor any instances of aggression or physical damage to our property and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems across all GLT locations and ensure that:

- we comply with the GDPR, effective 25 May 2018
- the images that are captured are useable for the purposes we require them for
- we reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- observing what an individual is doing
- taking action to prevent a crime
- using images of individuals that could affect their privacy

Principles

- A GLT location will only use surveillance cameras for the safety and security of that location and its staff, pupils and visitors.
- Surveillance will be used as a deterrent for violent behaviour and damage to the GLT location.
- The GLT location will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any classrooms or any toilet or changing facility.

- If the surveillance and CCTV systems fulfil their purpose and are no longer required, they will be deactivated.

Legal Framework

This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

CCTV and Insurance

Grove Learning Trust is part of the Department for Education's risk protection arrangement (RPA). Appendix 1 cross references these areas (CCTV and insurance through RPA) and provides a checklist to ensure compliance.

Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.

- **overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000
- **covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance

Grove Learning Trust does not condone the use of covert surveillance when monitoring the staff, students or volunteers. Covert surveillance will only be operable in exceptional and necessary circumstances.

Roles and Responsibilities

Data Controller

Grove Learning Trust is a corporate body, therefore, the Board of Trustees has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations. The Board of Trustees delegates day-to-day matters relating to data protection to the strategic operations leader and thus, for the benefit of this policy they act as the data controller.

The role of the data controller includes:

- processing surveillance and CCTV footage legally and fairly
- collecting, where necessary, surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly
- collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection
- ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary
- protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks

Data Protection Officer

The role of the data protection officer (DPO) includes:

- dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000
- ensuring that all data controllers across the different GLT locations handle and process surveillance and CCTV footage in accordance with data protection legislation
- ensuring that surveillance and CCTV footage is obtained in line with legal requirements
- ensuring consent, where it is required, is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR

- ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period
- keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request
- informing data subjects of how their data captured in surveillance and CCTV footage will be used by the specific GLT location, their rights for the data to be destroyed and the measures implemented by the GLT location to protect individuals' personal information
- preparing reports and management information on the location's level of risk related to data protection and processing performance
- reporting, where necessary to the highest management level e.g. the trust's board
- abiding by confidentiality requirements in relation to the duties undertaken while in the role
- monitoring the performance of the location's data protection impact assessment (DPIA) and providing advice where requested
- presenting reports regarding data processing at the GLT location to senior leaders and the Board of Trustees

Head Teacher

The role of the head teacher includes:

- meeting with the DPO to decide where CCTV is needed to justify its means
- conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage
- reviewing the *Surveillance and CCTV Policy* to ensure it is compliant with current legislation
- monitoring legislation to ensure the school is using surveillance fairly and lawfully
- communicating any changes to legislation with all members of staff

Estates Team

The role of the estates team includes:

- ensuring that the equipment is working correctly, including camera operation, clarity and view and effective recording and reporting any failures to the head teacher for budget consideration
- to achieve best practice, ensuring CCTV equipment is serviced annually and records of the service retained
- performance monitoring, including random operating checks, to be carried out, under the direction of the location's lead

Protocols

- The surveillance system(s) will be registered with the ICO in line with data protection legislation.
- The surveillance system(s) is (are) closed digital system which does not record audio.
- Warning signs must be placed in the location where the surveillance system is active, as mandated by the ICO's Code of Practice.
- The surveillance system has been designed for maximum effectiveness and efficiency; however, we cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.
- The surveillance system will not be trained on individuals unless an immediate response to an incident is required.
- The surveillance system will not be trained on private vehicles or property outside the perimeter of the GLT location.

Security

- Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected. The authorised CCTV system operators are the school's senior leaders, estates staff and the DPO.
- The main control facility is kept secure and locked when not in use.
- If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.
- Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.
- The DPO and head of the specific GLT location will decide when to record footage, e.g. a continuous loop outside the location's grounds to deter intruders.
- Any unnecessary footage captured will be securely deleted from the system.
- Any cameras that present faults will be repaired as soon as possible as to avoid any risk of a data breach.
- Ideally, the visual display of CCTV is accessible through a secure connection online connection, not just a single computer point of access.

Access

- Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.
- All sources containing images belong to, and remain the property of Grove Learning Trust.
- Individuals have the right to submit an SAR to the specific GLT location to gain access to their personal data in order to verify the lawfulness of the processing.
- The GLT location will verify the identity of the person making the request before any information is supplied.

- A copy of the information will be supplied to the individual free of charge; however, the location may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Requests by persons outside the GLT location for viewing or copying disks, or obtaining digital recordings, will be assessed by the location's lead such as the school's head teacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, within one month of receipt.
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded or excessive, we hold the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.
- In the event that a large quantity of information is being processed about an individual, the location will ask the individual to specify the information the request is in relation to.
- It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
- Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

    - the police – where the images recorded would assist in a specific criminal inquiry
    - prosecution agencies – such as the Crown Prosecution Service (CPS)
    - relevant legal representatives – such as lawyers and barristers
    - persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

- Requests for access or disclosure will be recorded and the location's lead will make the final decision as to whether recorded images may be released to persons other than the police.

Monitoring and Review

This policy will be monitored and reviewed on an annual basis.

The strategic operations lead, with DPOs, will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

The head teacher or location's leader will communicate changes to this policy to all members of staff.

Appendix 1 – CCTV and Insurance (RPA)

Equipment & Installation

- CCTV systems are securely installed and form part of the building's security infrastructure.
- Equipment is listed under Buildings, Contents, or Computers in asset registers.
- Outdoor cameras are weatherproof and securely mounted to prevent wind or rain damage (see Section 1 exclusions).

Security & Risk Management

- CCTV systems are included in the school's risk assessments.
- Systems are protected against unauthorised access (e.g. password-protected, firewalled).
- Regular checks are conducted to ensure cameras are operational and footage is being recorded.

Cyber & Data Protection

- CCTV systems connected to networks are included in the Cyber Response Plan.
- Staff with access to CCTV footage have completed NCSC cyber training.
- CCTV footage is stored securely and retained only as long as necessary.
- The school is registered with the Information Commissioner's Office (ICO) for data processing.

Documentation & Evidence

- CCTV systems are documented in the school's asset register.
- Maintenance logs and incident reports involving CCTV are kept.
- Any damage, theft, or cyber incident involving CCTV is reported to the RPA Third Party Administrator promptly.

Claims & Coverage Awareness

- Staff are aware that:
- - CCTV damage may be covered under Material Damage (Section 1).
- - Cyber breaches involving CCTV may be covered under Cyber (Section 14).
- - Data protection claims may be covered under Legal Expenses (Section 12) or Third Party Liability (Section 4).
- Claims are submitted via the RPA portal or contact details provided in the Claims Guidelines section.