

The Grove Partnership

CCTV POLICY

2025 - 2026



Previous Review:	June 2024
Date of this review:	July 2025
Comments:	Increased security and protection for staff who view footage, limited viewing in room locations & rationale for the viewing of historic footage.
Next review due by:	July 2026 (annual)
Review approved by Governing Body:	Shared with HR, Finance and Premises Committee via the Governor Hub on 17.07.2025 for meeting on 21.10.2025
Head teacher's Signature:	E. Patel

Contents:

1. Introduction.
2. Objectives of the CCTV system.
3. Responsibilities & operation of the system.
4. General statement of intent.
5. Control room (secure area).
6. Procedures for viewing purposes.
7. Recording media procedures.
8. Subject Rights of Access.
9. Complaints.
10. Public Information.
11. System maintenance.
12. Summary of key points.
13. Appendix A – Authorised Personnel (staff list & access rights)
14. Review of Policy
15. Links with other policies
16. Appendix B - Confidentiality statement for staff (viewing live images)
17. Appendix C – Confidentiality statement for parents/carers

CCTV POLICY

The Grove Partnership is committed to securing the safety and well-being of employees, pupils and others affected by activities on school premises.

1. Introduction:

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) systems at The Grove Partnership, hereafter referred to as 'the school'. It is intended to provide guidance as to good practice for users of the CCTV systems in School.

This Policy is based upon the Code of Practice published by the Information Commissioner, which sets out the standards that must be met if the requirements of the Data Protection Act 1998 and the General Data Protection Regulations (GDPR) are to be met.

2. Objectives of the CCTV System

- (a) To protect the school buildings and their assets both during and after school hours.
- (b) To provide improved site security to the inside of the building and the outside grounds.
- (c) To increase the personal safety of staff, pupils and visitors to reduce their fear of crime.
- (d) To support the provision of a safe environment for staff, pupils and visitors.
- (e) To act as a deterrent relating to vandalism and anti-social behaviour.
- (f) To support the Police in a bid to deter and detect crime.
- (g) To assist in identifying, apprehending and prosecuting offenders.
- (h) To protect members of the public and private property.
- (i) To assist in managing the school.
- (j) To support the safety and wellbeing of all staff.

- (k) To act as an internal investigative tool for incidents involving vandalism.
- (l) To prevent and identify bullying.
- (m) Ensuring that the school rules are respected so school can be properly managed.

The CCTV system will not be used to:

- Encroach on an individual's right to privacy.
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets)
- Follow particular individuals unless there is an ongoing emergency incident occurring.
- Pursue any other purposes than the ones stated above.

The list of uses for CCTV is not exhaustive and the other purposes may be or become relevant.

3. **Responsibilities and Operation of the System:**

The following management arrangements are in place:

- The persons who have been appointed to oversee the system and procedures are: Carol Jones/Chrissy Emerson.
- Their position within the school is: Business Manager(s).
- They will be responsible for: the use of the system through the formulation, development and implementation of appropriate policies and procedures; liaison with any security companies who operate or maintain the system; the point of contact for anyone with concerns or queries regarding its use or wishing to gain access to the footage such as the Police or members of the public. They will also be responsible for making sure that the data is only accessed by those with a genuine need to do so and with the appropriate authorisations (refer to Data Protection Policy located on the school website).
- The day-to-day operation and functioning of the CCTV system is the responsibility of the IT Manager.
- A CCTV download spreadsheet and access/release forms (external access) are stored on the school network (ICT Documents Drive) with restricted access to the ICT Manager and the School Business Managers.

Access to the CCTV Drive which stores the downloads, footage is restricted to those staff with full access rights identified in **Appendix A**.

4. **General Statement of intent**

The CCTV system and processes are checked with the Information Commissioner using their checklist which generates a report which provides an overall rating. The Grove Partnership are registered with the Information Commissioner under the terms of the Data Protection Act 1998 & General Data Protection Regulations 2018 (GDPR). The School will seek to comply with the requirements both of the Data Protection Regulations and Commissioner's Code of Practice. This is the responsibility of the Business Manager.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems in school and ensure that:

- We comply with the Data Protection Act 1998 and the General Data Protection Regulations 2018 (GDPR).
- The images that are captured are useable for the purpose 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.

These are listed below:

Data collected from surveillance & CCTV will be:

- Fairly and lawfully processed.
- Processed for limited purposes and not in any manner incompatible with those purposes.
- Adequate relevant and not excessive.
- Accurate.
- Not kept for longer than is necessary (incident downloads are retained whilst there is an ongoing pending investigation, and deleted once this is finalised).
- Processed in accordance with individuals' rights.
- Secure.
- Not transferred to countries without adequate protection.

The CCTV system and data is the property of the school.

The system comprises of a number of static and dome cameras located around the school sites.

Cameras will be used to monitor activities within the school, its grounds and other public areas to identify criminal activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and well-being of the school, together with its visitors. Camera images will be used as evidence in internal and external investigations into breach of codes of conduct, disciplinary issues, operational management and behaviour management. All staff, pupils, parents and carers will be informed of this intent by the publication of this policy on the school website.

Cameras are focused on public areas around the school sites. Cameras are not present in private areas such as toilets, medical rooms etc. Static cameras do not focus on private homes, gardens and other areas of private property. However, those cameras that encompass such areas, have privacy masks applied to them, to prevent footage being recorded of that private area.

Materials of knowledge secured as a result of CCTV will not be used for any commercial purpose. Information transferred using the appropriate media such as a USB drive or via secure encrypted email will only be used for the investigation of a specific crime or incident. Release to the media would only be allowed with the written authority of the police if this was required by them as part of a police investigation.

The planning and design of the system has endeavored to ensure that it will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

The school will notify visitors to the site of the use of CCTV by: Signage, as required under the General Data Protection Regulations which has been placed in areas covered by the school CCTV surveillance cameras (both interior and exterior of the building).

The school will notify new employees of the use of CCTV through the induction programme. This is the responsibility of the Business Manager.

CCTV images may only be viewed by authorised personnel. A list of staff currently authorised to access the system for the purposes of either **maintenance or observation** can be found at **Appendix A. This details the varied levels of authorisation.**

All such authorised staff will be required to sign a confidentiality agreement (See **Appendix B**).

Any images that are downloaded will be held in a secure location (restricted CCTV drive) and can only be accessed by those who are authorised to do so

5. Control Room

The CCTV recording equipment is currently held in room five (BBRD Site). It is stored in a secure, lockable metal cabinet. The Site Manager has a set of keys, which are held in the key safe.

Access to the monitor for the recording equipment is minimised to prevent unauthorised or inadvertent viewing. The IT Manager accesses the CCTV via a remote web interface.

Site	Monitor Location	Restrictions in place
Laurel Bank	A locked server unit in the Conference room.	No monitor in comms cabinet to avoid inadvertent viewing of cameras.
Broadbent Road	Locked in the server unit in room 5.	Screen is locked / switched off at all times,
Broadbent Road	Business Support access only. Staff & Visitor reception area.	The monitor is live view only of external areas including side roads and car park.
Broadbent Road	Business Support & Pastoral Staff. Pupil Reception area.	The monitor is live view only of external areas including side roads and car park.

Both of monitors are in staff only areas and are positioned in a way as to be not viewable by the public.

Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangements as outlined below.

Control Room Operators must satisfy themselves of the identity of any visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be denied.

Unless an immediate response to events is required, or in anticipation of an event occurring, staff in the CCTV control room must not direct cameras at an individual or a specific group of individuals.

The system may generate a certain amount of interest. It is vital that operations are maintained with minimum disruption. Casual visits to the control room to view footage will not be permitted. Visitors must first obtain written permission from the Head Teacher or other member of the Senior Leadership Team and must be accompanied throughout the visit.

Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

If out of hours emergency maintenance arises, the Control Room Operator/IT Manager must be satisfied as to the identity and purpose of contractors before allowing entry. The system is currently maintained by an approved contractor, via the local authority.

Other administrative functions include:

- Maintaining recordings.
- Maintaining occurrences / daily checks.
- Updated System maintenance logs.

6. **Procedures for viewing purposes**

Camera surveillance is operated 24 hours a day, every day of the year.

Information is held on the hard drive for a period of no more than 90 days. If information is required for evidence purposes it will be transferred to appropriate recording media.

Staff are authorised to view live CCTV live footage as part of their role solely to support the safety of the personnel on site. This forms part of the school safety and security measures in place.

All authorised third parties / members of staff who are allowed access or invited to view CCTV images **must** complete and sign Confidentiality Statement (**Appendix B**) before viewing takes place. This is located in the CCTV download and management pack.

Any parents/carers that are invited to view footage must complete and sign the CCTV Confidentiality and consent form for parents/carers (**Appendix C**) prior to viewing footage.

The CCTV download and management pack must be securely stored at night and during periods of school closure. This is the responsibility of the IT Manager.

All members of the Senior Leadership Team, The IT Manager and the Site Manager have access to log onto and access the CCTV system.

Members of the Senior Leadership Team are only permitted to review historic footage / playback footage in the SLT office at Broadbent Road and when there is at least one other member of SLT present when the system is accessed and footage is viewed.

If they have submitted a request to the IT Manager or Site Manager then the footage can be viewed in their offices.

The viewing of footage playbacks when an incident has occurred can only be undertaken by the IT Manager and Site Manager when a member of the Senior Leadership teams specifically requests them to do so and is present. This is to be done in either the IT Manager's office or the Site Manager's Office.

Members of the Senior Leadership Team are only permitted to view historic footage when they have a genuine reason to believe a crime has been committed, there is a risk to the health and safety of personnel in or around the building or an act of violence has occurred.

All Leaders who undertake this task must be able to provide a clear rationale for every request to view or access to footage.

The rationale for every viewing must be sent via email to SLT & the IT Manager to ensure there is appropriate viewing and transparency.

7. **Recording Media Procedures**

In order to maintain and preserve the integrity of the media used to record events from the hard drive and the facility to use them in any future proceedings, the following download procedures for external requests must be strictly adhered to:

- An incident download log is completed by the IT Manager.
- Where relevant, a crime number must be stated.
- Two identical copies of the incident will be saved as follows: - 1. Secure CCTV drive on the network, and 2. Issued to the external party.
- The top copy of the download log form will be provided to the Police or investigating organisation along with the released CCTV footage.
- The 'Archive Copy' will be retained in school, to be used as a back-up and must be held in a secure manner. This is stored in the archive file on the CCTV network.
- Upon completion of any investigation, the 'Archived footage' will be held for a period of time, no longer than necessary for any follow up investigations before being destroyed.
- Section 7 of the Incident Download log will be completed at the point of destruction.

8. Subject right of Access / Data Protection

Under the terms of the GDPR members of the public have a right to obtain confirmation that their personal information is being processed.

Individuals have a right to submit a SAR to gain access to their personal data in order to verify the lawfulness of the processing. Requests by persons outside the school for viewing or copying discs or obtaining digital recordings will be assessed by the Head teacher / Business manager in consultation with the DPO. This will be assessed on a case by case basis with close regard to data protection and freedom of information legislation. The school will verify the identity of any person making the request and this must be in writing before any information is supplied.

All requests will be responded to within one month of receipt.

In the event of numerous complex requests, the period of compliance will be extended. Releasing the recorded images to third parties will be permitted only in the following limited prescribed circumstances:

- Police; where the images would assist in a criminal enquiry.
- Prosecution agencies; The CPS.
- Relevant legal representatives; Solicitors, barristers.
- Insurance companies.

All third parties must complete a confidentiality agreement and CCTV access form.

Recordings are stored for a period of no more than 90 days before being overwritten. If the archive period has elapsed before the application is received, the information may have been overwritten and the application cannot be processed.

Access to recorded images is restricted to those staff who have need of access in order to comply with the objectives of the system.

Any request for copy recordings should be made in person at the address where the CCTV system is located. Strict controls relating to confidentiality are applied throughout all procedures in compliance with the requirements of the Data Protection Regulations.

Any requests for Data Subject Access should be made by application to the Head Teacher/Business Manager and will be processed in accordance with the procedures as set out in the Management Pack.

9. Complaints

Any complaints about the school's CCTV system should be addressed to the Head Teacher/Business Manager. Complaints will be investigated in accordance with the Schools Complaints Procedure.

10. Public Information

Copies of this Policy are available on the school website.

11. System Maintenance

The IT Manager will check and confirm the efficiency of the system on a daily basis to ensure that the time and date are correct, that the recording equipment is operating correctly and that cameras are functional.

Checks will be logged in CCTV Maintenance spreadsheet, stored on the school network. Any faults detected will be notified immediately to the Business Manager.

A regular maintenance programme is in place and will be carried out in accordance with an agreed schedule by an approved contractor. The IT Manager is responsible for making sure that the annual maintenance check is undertaken and completed satisfactorily.

Hard drives are fixed units and would only be removed from site for the purposes of repair and maintenance by approved contractors.

Equipment and recordings may be viewed by personnel authorised to undertake installation and maintenance of the CCTV systems. Such viewing will be restricted to that necessary for system work.

During times of school closure, the CCTV system will continue to operate as normal.

Summary of Key Points:

- This policy will be reviewed annually.
- The CCTV system is owned and operated by the school.
- The CCTV system is not open to visitors except by prior arrangement and legitimate reason.
- Liaison meetings may be held with the Police and other bodies.
- Recording media used will be properly indexed, stored and destroyed after appropriate use.
- Recording media may only be viewed by authorised school personnel and the Police.
- Records will not be made available to the media for commercial or entertainment purposes.
- Any breaches of the Code will be investigated by the Head Teacher. An independent investigation will be carried out for serious breaches.

- Regular reviews of the systems operation will take place and any necessary changes in procedure or camera siting/position will be implemented.

This policy is based on: the following Legislation:

[UK General Data Protection Regulation](#)

[Data Protection Act 2018](#)

[Human Rights Act 1998](#)

[European Convention on Human Rights](#)

[The Regulation of Investigatory Powers Act 2000](#)

[The Protection of Freedoms Act 2012](#)

[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](#)

Appendix A



Kingsland School

AUTHORISATION PERSONNEL

The following staff are authorised to view the CCTV images

Post Title	Current Post holder	Reason for Authorisation	Level of Authorisation
Head Teacher	Emmett Patel	Head Teacher	Full authorised access to the CCTV surveillance & recording system in line with stipulations in section 6.
Head Of School (BBRD)	Karl Said	Day to day running of the school.	Full authorised access to the CCTV surveillance & recording system in line with stipulations in section 6.
Assistant Head Teacher	Kayleigh Bell	Day to day running of the school.	Full authorised access to the CCTV surveillance & recording system in line with stipulations in section 6.
Head of School (LB)	Sal Qureshi	Day to day running of the school.	Full authorised access to the CCTV surveillance & recording system in line with stipulations in section 6.
Assistant Head Teacher	Hammad Nazir	Day to day running of the school.	Full authorised access to the CCTV surveillance & recording system in line with stipulations in section 6.
Business Manager(s)	Carol Jones Chrissy Emerson	Responsibility for the system and Data Controller.	Full authorised access to the CCTV surveillance & recording system in line with stipulations in section 6..
IT Manager	Craig Perry	Maintenance and operation.	Full authorised access to the CCTV surveillance & recording system in line with stipulations in section 6.
Business Support Team (Reception)	Kelly Moore Fiona Harrison Zoe Tindall Lauren Heaton	Safety & Security: view incidents of disruption/vandalism & inform members of SLT.	Live footage view only (restricted areas: pupil entrance/lobby & school carl park).

Pastoral Team (Pupil reception)	Danny Smith Helen Howard-Smith Kelly Deumlich Chloe Emerson	Safety & Security: view incidents of disruption/vandalism & inform members of SLT.	Live footage view only (restricted areas: pupil entrance/lobby & school car park).
Site Manager	Paul Hough	Safety & Security: view incidents of disruption/vandalism & inform members of SLT.	Live footage view & Playback
Chair of Governors & Vice Chair of Governors	Appointed Chair of Governors & the appointed Vice Chair	As part of an investigation & to view incidents when requested to do so by the Head teacher.	View downloaded CCTV footage.

CCTV - CONFIDENTIALITY STATEMENT

To be completed by all staff who view live images

Name: **(Please Print)**

Post: **(Please Print)**

I THE UNDERSIGNED:

(DELETE AS APPROPRIATE)

- AM AUTHORISED TO VIEW CCTV FOOTAGE IN THE COURSE OF MY PROFESSIONAL DUTIES AT THE GROVE PARTNERSHIP **or** I AM AUTHORISED TO VIEW CCTV AS PART OF AN INVESTIGATION.
- AM AUTHORISED TO VIEW LIVE CCTV FOOTAGE ONLY IN THE EVENT OF INCIDENTS OF VANDALISM/VIOLENCE/BREACH OF SECURITY.
- AGREE THAT ANY INFORMATION THAT I HAVE ACCESS TO DURING THE COURSE OF ANY VIEWING WILL REMAIN IN CONFIDENCE UNDER THE TERMS OF THE DATA PROTECTION ACT 1998 & GENERAL DATA PROTECTION REGULATIONS 2018 (GDPR)
- CONFIRM THAT I HAVE READ AND UNDERSTAND MY ROLE AND RESPONSIBILITIES AS SET OUT IN THE SCHOOL CCTV POLICY

Signed:

Job Title:

Date:

Approved by: (Head teacher)

Date:

Appendix C

CCTV - CONFIDENTIALITY & CONSENT FORM (parents/carers)

Name: (Please Print) _____

Connection / Link to School: i.e. parent/carer _____

Enter the details to evidence on what ground individuals are permitted to view CCTV footage: *e.g incident, include details such as date, time & location.*

I UNDERSTAND:

- There are appropriate policies and procedures in place at The Grove Partnership for anyone using or wishing to gain access to the footage such as the Police or members of the public.
- The Business Manager is responsible for making sure that the data is only accessed by those with a genuine need to do so and with the appropriate authorisations.
- The CCTV system and data is the property of the school and will remain so.
- Camera images will be used as evidence in internal and external investigations into breach of codes of conduct, disciplinary issues, operational management and behaviour management.
- All staff, pupils, parents and carers will be informed of this intent by the publication of this policy on the school website.
- All personnel/members of the public/parents/carers approved to view footage are required to read and sign this form to ensure that there are reasonable grounds to view the footage and that confidentiality is maintained.
- We protect the rights of other individuals who are present on CCTV footage.
- All parties will sign their consent before footage is viewed.
- We will not release images but allow for controlled viewing on site.
- Recording media may only be viewed by authorised personnel or as part of an investigation around behavior/criminal damage/violent incidents/security breaches. This will be approved by the Head teacher.

I agree that any information that I have access to during the course of viewing will remain in confidence under the terms of the data protection action 1998 and general data protection regulations 2018 (GDPR).

I confirm that I have read and understand all of the above.

Signed: Date:

Approved by:(Head teacher) Date:

Links with other Policies:

The Grove Partnership is committed to the Health and Safety of all its staff and pupils, and we believe that we must always take action to safeguard the well-being of all concerned. This policy, therefore, links closely with the following:

- Safeguarding & Child Protection Policy
- Staff Behaviour (Staff Handbook)
- Staff Code of Conduct Policy
- Anti-Bullying Policy
- Improving Behaviour Policy
- Data Protection Policy.

Review of Policy:

This policy was formally adopted by The Grove Partnership in July 2014, is renewed annually and replaces all previous policies, procedures and guidelines in use within the establishment.

Reviewer(s): Carol Jones

Reviewer(s): C Emerson & C. Perry

Reviewer(s): C Emerson

Reviewer(s): C Emerson & C. Perry

Reviewer(s): C Emerson & C. Perry

Reviewer(s): C Emerson & C. Perry

Reviewer(s): C Emerson & C. Perry

Reviewer(s): C. Perry

Reviewer(s): C Emerson & C. Perry

Reviewer(s): C Emerson & C. Perry

Reviewed: October 2017

Reviewed: October 2018

Reviewed: October 2019

Reviewed: November 2020

Reviewed: November 2021

Reviewed: October 2022

Reviewed: February 2023

Reviewed: September 2023

Reviewed: June 2024

Reviewed: July 2025