



King's Academy
Rowner

CCTV Policy

| | | | |
|----------------|------------------|------------------|------------|
| Approved by: | LGB | Date: | 30.4.2025 |
| Maintained by: | Georgina Mulhall | Next review due: | April 2026 |



Contents

| | |
|--|---|
| Objectives | 1 |
| Purpose of This Policy | 2 |
| Statement of Intent | 2 |
| System Management | 2 |
| Downloading Captured Data Onto Other Media | 3 |
| Complaints About the Use of CCTV | 3 |
| Requests for Access by the Data Subject | 4 |
| Appendix 1 - Locations of cameras | 4 |

Objectives

The academy recognises that CCTV (closed-circuit television) systems can be privacy intrusive. The purpose of the CCTV system is to assist the academy in reaching the following objectives:

- A. To protect pupils, staff and visitors against harm to their person and/or property;
- B. To increase a sense of personal safety and reduce the fear of crime;
- C. To protect the academy buildings and assets;
- D. To support the police in preventing and detecting crime;
- E. To assist in identifying, apprehending and prosecuting offenders;
- F. To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence; and
- G. To assist in managing the academy.

Purpose of This Policy

The purpose of this policy is to regulate the management, operation and use of the CCTV system at the academy. CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilet cubicles, changing facilities, etc.

Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Signs are prominently displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of the purposes for which CCTV is used.

The CCTV system will seek to comply with the requirements of both the Data Protection Act and the most recent Commissioner's Code of Practice.

The Academy will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act. The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.



The planning and design have endeavoured to ensure that the system 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.

Warning signs, as required by the Code of Practice of the Information Commissioner, will be clearly visible on the site.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception. CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 30 days.

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. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

System Management

Access to the CCTV system is in the Administration Office next to the SLT Office. The CCTV has a digital code to protect the screen.

The CCTV system will be administered and managed by KGA Hampshire IT Team who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager, the system will be managed by Mr Mark Riley.

The system and the data collected will only be available to the Systems Manager, their replacement and appropriate members of the senior leadership team as determined by the Executive Headteacher. The CCTV system is designed to be in operation 24 hours each day, every day of the year, though the academy does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that the cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by providing clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above requests access to the CCTV data or system, the System Manager must satisfy themselves of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

Details of all visits and visitors will be recorded in a system logbook, including time/data of access and details of images viewed and the purpose for so doing.

Downloading Captured Data Onto Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures:

- A. Each downloaded media must be identified by a unique mark.
- B. Before use, each downloaded media must be cleaned of any previous recording.
- C. The System Manager will register the date and time of downloaded media insertion, including its reference.
- D. Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a



later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.

- E. If downloaded media is archived, the reference must be noted.
- F. If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable, if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remain the property of the academy and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The academy also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the academy to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the academy's Data Protection Officer and a decision made by a senior leader of the academy in consultation with the academy's Data Protection Officer.

Complaints About the Use of CCTV

Any complaints in relation to the academy's CCTV system should be addressed to the Executive Headteacher.

Requests for Access by the Data Subject

The academy recognises the rights of individuals under data protection law to access data held about themselves, including CCTV footage. However, if the requested footage contains images of other identifiable individuals, the academy must balance the data subject's right of access against the privacy rights of others. The academy's current CCTV systems do not necessarily have the technical capability to redact footage to remove or obscure other individuals. Therefore, in cases where redaction is not possible, the academy may not be able to release the requested CCTV footage.

Where appropriate, the academy may provide still images that have been redacted, if feasible. All such requests will be reviewed carefully in consultation with the academy's Data Protection Officer to ensure compliance with UK data protection law.

Appendix 1 - Locations of cameras

A copy of this table is stored separately from this policy and kept as a working document for reference.

| Camera Type | Location | Sound | Recording Capacity | Swivel/Fixed |
|-------------|----------|-------|--------------------|--------------|
| | | | | |



| | | | | |
|--|--|--|--|--|
| | | | | |
|--|--|--|--|--|