ENFIELD GRAMMAR SCHOOL

CCTV POLICY

Committee	Resources and Management
Date Approved	September 2024
Review Date	September 2025

Contents

Introduction and Objectives

A Closed-Circuit Television System (CCTV) is in place at Enfield Grammar School ("the School") comprising a number of fixed cameras. All cameras are fully operational.

The owner of the system is the School.

For the purposes of the UK Data Protection Legislation, the data controller is the School, which is registered with the Information Commissioner, registration Z2726034.

The system manager is the Premises Manager, the Finance and Operations Manager is the key contact point, and should be contacted via the school's normal contact details on the website for any issues relating to the system.

It is recognised that operation of the School's CCTV System may be considered to infringe on the privacy of individuals. The School recognises that it is their responsibility to ensure that CCTV on the premises should always comply with all relevant legislation, to ensure its legality and legitimacy. CCTV will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well-being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.

The legislation concerning CCTV in Section 30 of the Protection of Freedoms Act 2012 has produced a CCTV Code of Practice from the Surveillance Camera Commissioner that has been approved by Parliament and the School must pay due regard to the code.

The School, in managing its CCTV operations under this Code of practice, will endorse and comply with all 12 guiding principles of the Surveillance Camera Code of Practice.

The Codes of Practice and observance of the Operational Procedures contained in the policy shall ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial.

The School CCTV System shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

The objectives of the School CCTV System which form the lawful basis for the processing of data are: –

- To help deter crime and reduce the fear of crime.
- To ensure the safety of persons in or near our premises and vehicles.
- To protect our property from theft, vandalism and other threats.
- To help detect crime and disorder, or other public safety issues.
- To provide evidential material suitable for court proceedings, dispute resolution and civil proceedings.
- To assist in supporting civil proceedings.
- To assist in the overall management of the School, including dispute resolution and discipline management.

Responsibilities

Governing Body

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

The Headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system.
- Ensure that the guidance set out in this policy is followed by all staff.
- Review the CCTV policy to check that the school is compliant with legislation.
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection.
- Sign off on any expansion or upgrading to the CCTV system.
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties.
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified.

Operation

The CCTV system will be operational 24 hours a day, 365 days a year.

The system will not record audio.

Recordings will have date and time stamps. This will be checked by the Premises Manager termly and when the clocks change.

Notification

- A copy of this CCTV Policy will be provided on request to staff, students, parents and visitors to the school and will be made available on the school website.
- The location of CCTV cameras will also be indicated and adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation.
- Adequate signage is prominently displayed at entrances to the school buildings and around the premises where CCTV is in operation.

Procedures

A member of the schools leadership team will provide access to the system where this is required. The Premises Manager, Wellbeing and Safeguarding Manager and Duty Manager also have access to the system.

Recordings will only be accessed where an incident has occurred or is suspected which falls within the objectives above. Review of recordings will take place only under supervision, and export of recordings will only be permitted where there is a legal requirement to do so. The persons involved in an incident may be present to review the information (including pupils) where this is deemed necessary.

The single camera on the entrance gates will be visible at all times at Reception, where it will be used to check on visitors before entry. The receptionists will have access only to the live feed.

A record will be made of all uses of recordings and who viewed them.

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 60 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recording will be redacted (identifiable information such as faces blurred) when requested as part of a Subject Access Request.

Security

- The system manager will be responsible for overseeing the security of the CCTV system and footage.
- The system will be checked for faults once a term by the Premises Manager. Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure.
- Footage will be stored securely and encrypted wherever possible.
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use.

How we comply with the code

Principle 1 - Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

The specific purposes are given in Objectives above. There is a pressing need for the School to ensure the safety of its staff pupils and visitors, and to protect its assets.

Principle 2 - The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

This has been carefully considered. Fixed cameras record continuously within their scope and public areas are excluded, as much as possible, from scope.

Cameras are not placed in enclosed areas where there is an expectation of privacy e.g. changing rooms and private areas of bathrooms.

Principle 3 - There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

This is provided by this policy.

Principle 4 - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

The School Business Manager is responsible and accountable for all activities.

Principle 5 - Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

These are provided by this policy.

Principle 6 - No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

Recordings made by detection are deleted after 30 days unless action is taken to preserve them. This is only done where the recordings are required for one of the objectives noted above.

Principle 7 - Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

Only the roles noted above can access images except where required by law enforcement. The roles noted above will manage the viewing of images in normal use to meet the objectives above. Viewing of images by persons involved in incidents will be granted where necessary for the objectives.

Principle 8 - Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

These have been considered. As a technical standard, we have a minimum image size of 1080p to ensure sufficient clarity.

Principle 9 - Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

Images are stored on the servers at the school. These are appropriately secured.

Principle 10 - There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

This policy is reviewed annually, the review date is at the end. No reporting is considered necessary by the governors except for logging of details of individual accesses for the purposes.

Principle 11 - When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

This principle is supported by this document.

Principle 12 - Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

No reference databases are used.