SWANLEA SCHOOL

CCTV Policy

Reviewed: Sept 2022 by Sam Cullen (SBM), Ali Ashraf (Buildings and Resources Manager)
Approved by: Goes to Resources 14.11.22
Next review date: Oct 2025

1. Introduction

CCTV cameras are now a familiar sight throughout the country. They are one of the many measures being introduced to help prevent crime and make communities safer places to live, work and visit.

Some schools have expressed concern that parts of their premises are vulnerable to anti-social behaviour and criminal activity, especially out of school hours.

The possibility of vandalism, arson and burglary in schools is of concern to all, whether we are Teachers, Governors or Parents. Whilst our record of prevention in Tower Hamlets is good, we all acknowledge the requirements for greater measures to ensure the welfare of all who use our schools and the need for a safe and secure environment in which to work.

CCTV systems are carefully planned and are designed to provide evidential quality images. These images will usually cover vulnerable areas and access points. The location of each camera is individually accessed and positioned in order to provide specific images e.g. camera one; identity images of vehicles entering site.

However, the system fitted must effectively meet the operational requirement set for it. If it does not do this, then it is not fit for use and fails to meet its stated registered CCTV purpose under data process legislation. It is also illegal for systems to impinge upon individual privacy.

The purpose of this Policy is to ensure that this does not occur.

2. Reasoning

The Policy has been agreed by the Governing Body and we firmly believe in its value in making CCTV systems a success.

The attention to security and crime/antisocial preventative measures will help to keep schools safe and enjoyable environments. Where funds and vital resources are targeted on maintaining and developing the quality of teaching and learning environment, where they are needed most, and not on replacing stolen and vandalised equipment or property.

3. Legal Framework

Legal framework This policy has due regard to legislation and statutory guidance, 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 (GDPR) (2018)

- The Data Protection Act 2018
- 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'
- Information Commissioner's Office (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'

4. Details

Name of Data Controller: The School Business Manager – Samantha Cullen

This Policy has been drawn up and agreed by the Governing Body; it governs the activities of those involved in the operation and installation of a School CCTV System.

The Policy will follow the guidelines published by the Home Office and the Information Commissioners Office (ICO) 2008 on the use of CCTV in public places and we adhere to the Freedom of Information Act (FOI) 2000 and Surveillance Camera Code of Practice.

This will be a document subject to on-going evaluation and review.

5. Definition

The system is owned by Swanlea Secondary School within the London Borough of Tower Hamlets.

Camera positions have been carefully located, to ensure they are appropriate and effective whilst minimising any collateral intrusion. It is impossible, however, to ensure that every incident will be seen or recorded.

The CCTV system will be maintained in accordance with the Data Commissioner's CCTV code of practice guidelines (2008) and this policy.

The CCTV system will be maintained and reviewed according to the guidelines; all recording equipment will be regularly tested for clarity of images.

Maintenance checks

1. Cameras must be checked once a week to ensure that they are operational
2. Recorders must be checked once a month to ensure that they are recording and it is possible to down load images.
3. Camera fixings must be checked to ensure safety and security, during planned maintenance e.g. cleaning cameras
4. Repairs will be made to the system within two weeks if practical, dependent upon cost and CCTV review

School CCTV systems may comprise both external and or internal cameras, within the site.
Positions of the cameras will be detailed in the school's impact assessment and the operational requirement for the CCTV system, held by the Data Controller.

Camera images are recorded and displayed on a CCTV monitor in the Premises office. The recording media is DVR. Images recorded on a DVR are stored on a hard drive, which is automatically overwritten after a set period of time.

Operation of the system is controlled by the school's Data Controller.

6. Purpose of CCTV

The system overall is intended to provide and promote a safe secure environment for pupils and for those who work or use the facilities of the school and to protect the school buildings and resources. It is hoped that it will also reduce the fear of crime and anti-social behaviour within the location.

It shall be used for the purpose of:

- preventing and deterring crime & antisocial behaviour
- student, staff and public safety
- assisting responsible agencies in the investigation of crime & antisocial behaviour
- where appropriate staff & student discipline issues and general facilities management.

It will achieve this by:

- providing evidential quality images of criminal incidents and suspects,
- assisting the responsible authorities in the investigation of crime & disorder.

The system is intended to view and monitor activity in the immediate area of the school only.

7 Data Protection

The system shall be used in accordance to all relevant laws and guidelines, including the Data Protection Act 1998, Surveillance Camera Code of Practice, The Human Rights Act 1998, Freedom of Information Act 2000, GDPR May 2018 and if appropriate Regulation of Investigatory Powers Act 2000.

Where appropriate, safeguards have been installed to prevent cameras focusing on peoples' homes, gardens or other areas of private property (collateral intrusion).

Obviously similar safeguards are used to limit any collateral intrusion of inappropriate locations within the school as well.

8. Signage

Signs will be displayed at entrance points and within the area covered by the system to inform staff, students and the public. Signs will detail the ownership of the system where this is not obvious and an appropriate contact number for the Data Controller.

9. Management of the system

The overall management of the system is the responsibility of the Governing Body of the school, who will normally appoint the Head teacher or their nominee to act on their behalf and carry out the function of Data Controller.

10. Management and Operation of Control Equipment

The system will be managed in accordance will all relevant legislation.

Access and Security

The day-to-day management and security of the control equipment and data is the responsibility of the Data Controller who will follow the data protection guidelines with regard to access to the 'Control Room' by visitors. Failure to do this may result in criminal proceedings.

Care must be taken to ensure that unauthorised person/s, are not able to see the screen images produced by the system. This does not mean that certain camera images may not be fed to specific users, e.g. door entry views to the reception desk. Access to images is only authorised by the Data Controller and images are not shared with 3rd parties (except for law enforcement bodies).

Incident Reporting

An incident log/book shall be stored in a secure lockable place, and is maintained by the Data Controller so details of any incidents relating to the use of the system are logged. Written records will be signed and dated by the Data Controller.

Incident Response

During monitoring if **criminal or suspicious activity of a serious nature** is observed then the school should immediately inform the Police. Once an incident is reported to the Police it will be dealt with in accordance with Police procedure.

All other incidents will be logged and dealt with by the relevant authorities.

Recording of Events

All cameras, monitors and recording equipment will be checked regularly to ensure that they are in working condition (see above) and able to fulfill this role.

A record of image usage and storage must be maintained. An automatic time/date generator must be incorporated on all recoding equipment. It is acknowledged that identification for successful prosecution may prove difficult solely from recorded events and efforts should always be made to provide additional verification of incidents.

Systems using Digital Recording & media storage

Digital Recording Protocol

Digital Recording is a continuous operation with the images automatically stored on the hard drive, which is overwritten after a set period of time (usually 28 days). Any images are stored on the hard drive for authorized personnel to view. After an incident has been resolved, the digital images are deleted. If the Police request any images, they save them onto their own memory sticks.

Only authorized staff will have access to the system and the down loaded images.

Storage of Recorded Images

- The storage space shall be dust and moisture proof.
- Only authorised staff will have access to stored media
- A register shall be maintained to log the use of all images stored and viewed and must be kept in a secure place.
- Any stored images will be kept in secure storage for a maximum period of 1 month
- Any images used/sored for an investigation shall be deleted once the investigation has concluded.

Memory Sticks as Evidence

- Any memory stick that is to be used as evidence in any Court action must be of proven integrity.
- There must be evidence of continuity of handling of the memory stick from the time it was first brought into use to its production in Court as evidence.
- The memory stick evidence must be the original recording. There must be no editing, either by cutting or splicing or recording from other sources.
- There shall be clear evidence that the memory stick was new or had been erased prior to use.
- When the Police have requested access to a recording, no member of the school or Council staff shall play back or make any use of the required images/recording.
- When removing an original image onto memory stick for recording evidence, the Police Officer shall comply with normal Police procedures for the removal, copying and retention of the memory stick.
- In all cases the reviewing of memory sticks shall be carried out under the Data Controller's supervision at an agreed location.

- All such access shall be recorded in the 'recordings being viewed' register.
- In the event of a major incident, emergency access to images/recordings would be made available to any authorized Police Officer.
- A request to view a recording not mentioned above must be agreed by the Headteacher or Data Controller.

DISPOSAL OF memory sticks

- When memory sticks are disposed of in addition to ensuring that all images have been permanently wiped they will be destroyed by secure methods.

Viewing and copying of images by appropriate personnel

- Viewing or copying will be carried out only if it would assist in the school services for which the Headteacher is responsible or to address one of the issues stated in the 'purpose of CCTV'.
- The Governors and Headteacher are not to take recorded images away from the school premises under any circumstances.
- A record of viewing and copying must be noted in the register.
- Memory sticks will be returned to secure storage immediately after viewing.

THE REGISTER OF INCIDENTS AND REVIEWS

The register will include the following:

- When searching or reviewing an incident the purpose of doing so should be recorded. Also note if the search was successful or not
- Who carried out search and/or copied of the event,
- Persons present (particularly when reviewing)
- Date, start and end time of the incident.
- Date and time of the review/copy.
- Details of the officer or authorised agent, collecting the copied media and their contact details.
- Date of collection along with a signature and name in block capitals, including agency.
- On occasion where the request relates to an ongoing incident or investigation any appropriate reference numbers should also be included.
- If appropriate number of disks or copies supplied.

11 ACCESS TO RECORDED INFORMATION

- The Data Protection Act provides Data Subjects (individuals to whom "personal data relates") with a right to have access to their personal data held by an organisation, this also include CCTV images relating to them. People can make a request to view their footage by making a Subject Access

Request. Subject Access Requests must be made in writing on the form available from the school. Where Subject Access Requests are made on behalf of a data subject, a written signed consent will be required from the data subject before the access to the footage is provided. In all cases, the Data Controller must be careful not to disclose footages of other third party individuals without their prior consent. If consent is not given and images are not able to be shown without 3rd parties then footage may not be possible to be viewed.

- Applications received from outside bodies (e.g. solicitors) to view or release recorded data will be referred to the Head teacher. In these circumstances recordings will normally be released where satisfactory documentation is produced showing they are required for legal proceedings, or a Court Order.

- A fee will be charged for the provision of stored data, £10.00 for subject access requests and a sum not exceeding the cost of materials in other cases.

- CCTV recordings are overwritten after 28 days. Should a recording be required to be kept, parents and authorised persons must request for this writing 10 days of the incident occurring. The school will undertake to keep a recording of the incident for 30 days and after this date, the recording will be destroyed if no longer required.

12. STAFF TRAINING

- A requirement under the CCTV code of practice is that personnel responsible for the system know how to manage the data and access the images.
- The effectiveness of the system depends on the quality of personnel selected for its operation.
- The Headteacher shall ensure that all appropriate staff are trained on the use of the equipment and familiar with their data protection responsibilities as detailed in the ICO's CCTV code of practice 2008

13. COMPLAINTS

- Any complaints about the school's CCTV system should be addressed to the Head teacher.
- Complaints will be investigated in accordance with Section 7 of this Policy.

14. BREACHES OF THE POLICY

- Misuse of recorded imagery or the system will be a disciplinary offence
- Any breaches of the Policy by school staff will be individually investigated by the Headteacher, in order for him/her to take the appropriate disciplinary action
- Disciplinary action may also include prosecution under the Data Protection Act and criminal proceedings may ensue.

15. REVIEW OF POLICY

Reviewed: Sept 2022 by Sam Cullen (SBM), Ali Ashraf (Buildings and Resources Manager)
Approved by: Goes to Resources 14.11.22
Next review date: Oct 2025

- This Policy will be reviewed every three years unless there is a change to legislation in the interim.

Swanlea School

Register of CCTV Incidents and reviews (Sample)

CONFIDENTIAL

CCTV Incident Log

Date of Search
Reason for Search:
Successful? YES / NO
Who Searched?
Present: Head Teacher/or SLT only
Name:
Date and Time Of incident:
Camera Details:
Filed to desktop in CCTV room? YES / NO

Reviewed: Sept 2022 by Sam Cullen (SBM), Ali Ashraf (Buildings and Resources Manager)
Approved by: Goes to Resources 14.11.22
Next review date: Oct 2025

Police Reference Number – if applicable
Action recorded
Action Taken :
Date footage removed:

Copy of incident received by_____ Date_____

Signed_____

On behalf of_____Organisation

Authorised by_____

Checked by_____ Data Controller

Reference Number_____

Reviewed: Sept 2022 by Sam Cullen (SBM), Ali Ashraf (Buildings and Resources Manager)
Approved by: Goes to Resources 14.11.22
Next review date: Oct 2025