Smithy Street Primary School

CCTV Policy

Approved by staff and governors

July 2018

POLICY FOR USE OF THE CCTV SYSTEM AT SMITHY STREET PRIMARY SCHOOL

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 only cover external 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 meet effectively 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.

The Policy has been agreed by the London Borough of Tower Hamlets, the Governing Body and the Metropolitan Police 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.

1. INTRODUCTION

This Policy has been drawn up and agreed between the Governing Body, the London Borough of Tower Hamlets and the Metropolitan Police; 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.

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

2. DEFINITION OF THE SYSTEM

The system is owned by Smithy Street Primary School within the London Borough of Tower Hamlets.

Camera positions have been carefully located, to ensure they are appropriate and effective whilst minimizing 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 Commissioners 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 tested for clarity of images.

Maintenance checks

1. Cameras must be checked regularly 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, dependant 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 Manager's Office. 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.

3. 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.

4. DATA PROTECTION

The system shall be used in accordance to all relevant laws and guidelines, including the Data Protection Act 2018, GDPR (General Data Protection Regulation) and The Human Rights Act 1998 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.

5. SIGNAGE

Signs will be displayed at entrance points and within the area covered by the system to inform staff, students and the public.

6. 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.

7. 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.

Incident Response

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.

An automatic time/date generator must be incorporated on all recording 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.

Digital Recording Protocol

Digital Recording is a continuous operation with the images automatically stored on the hard drive, which is overwritten after a period of time. The storage capacity of the hard drive is dependent on the number of cameras, quality of images and size of drive.

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

Storage and Retention of CCTV images

Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

All retained data will be stored securely.

Downloaded media as Evidence

- Any downloaded media 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 downloaded media from the time it was first brought into use to its production in Court as evidence.
- The downloaded media 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 downloaded media 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 downloaded media.

- When removing an original downloaded media for recording evidence, the Police Officer shall comply with normal Police procedures for the removal, copying and retention of the downloaded media.
- In all cases the reviewing of downloaded media shall be carried out under the Data Controller's supervision at an agreed location.
- In the event of a major incident, emergency access to downloaded media would be made available to any authorized Police Officer.
- A request to view the downloaded media not mentioned above must be agreed by the Headteacher or Data Controller.

Disposal of downloaded media

- When downloaded media 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.

8. SUBJECT ACCES REQUEST

- The Data Protection Act 2018 and GDPR (General Data Protection Regulation) 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.

- 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.

- Under the Data Protection Act and GDPR (General Data Protection Regulation) there will be no fee charged for the provision of stored data.

9. 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 famulure with their data protection responsibilities as detailed in the ICO's CCTV code of practice 2008

10. COMPLAINTS

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

11. 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

12. REVIEW OF POLICY

- This Policy will be reviewed at least every 2 years.