HORNCHURCH HIGH SCHOOL
EXCELLENCE FOR ALL

POLICY FOR USE OF CCTV SYSTEM

Rationale

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. HHS like many schools has expressed concern that parts of their premises are vulnerable to anti-social behaviour and criminal activity, especially out of school hours. Indeed the possibility of vandalism, arson and burglary in schools is of concern to all, whether we are teachers, governors or parents.
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
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 attention to security and crime/antisocial preventative measures will help to keep HHS a safe and secure environment. This will mean that 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.

1.1 INTRODUCTION

The Policy follows the guidelines published by the Home Office and the Information Commissioners Office (ICO) 2008 on the use of CCTV in public places. This document is subject to on-going evaluation and annual review.

1.2. DEFINITION OF THE SYSTEM

The system is owned by HHS .
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 and all recording equipment tested on an on-going basis for clarity of images .

Maintenance checks
For the Main School system:
The Site Manager will be responsible to see that:
1. Cameras are checked daily to ensure that they are operational
2. Recorders are checked daily to ensure that they are recording and images can be down loaded.

3. Camera fixings are checked to ensure safety and security during planned maintenance e.g. cleaning cameras
4. Repairs will be made to the system within a week whenever possible.

The School CCTV systems comprise both external and or internal cameras within the site.
Camera images are recorded and displayed on a CCTV monitor in the IT office and the Site Manager's Office. The recordings are stored on the School's servers and are automatically overwritten after a set period of time.

1.3. PURPOSE OF CCTV

The system overall is intended to provide and promote a safe secure environment for students 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;
- supporting 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.

1.4. DATA PROTECTION

The system shall be used in accordance to all relevant laws and guidelines, including the Data Protection Act 1998, 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).
Similar safeguards are used to limit any collateral intrusion of inappropriate locations within the school as well.

1.5. SIGNAGE

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

1.6. 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. This role is undertaken by the Site Manager, when present and the IT Network Manager when not .

1.7. 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 Site Manager who follows the data protection guidelines with regard to access to the Control Screens by visitors. Failure to do this may result in criminal proceedings. Care is taken to ensure that unauthorised person/s, are not able to see the screen images produced by the system.

Incident Reporting
All incidents should be reported to the Site Manager / IT Network Manager by email.
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.
Recording of Events
All cameras, monitors and recording equipment are checked regularly to ensure that they are in working condition (see above) and able to fulfil this role.
An automatic time/date generator is 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 set 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.
Prior to recording, the equipment shall be checked to ensure it is in good working order.

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.
Requests to view or copy must be made by email to the Site Manager/ IT Network Manager

1.8. 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.

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.

1.9. 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 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

10. COMPLAINTS

Any complaints about the schools CCTV system should be addressed to the Head teacher.
Complaints will be investigated in accordance with the Albany School Complaints 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 or nominated Investigating Officer, in order for them to take the appropriate disciplinary action .
Disciplinary action can also include prosecution under the Data Protection Act and criminal proceedings .

Appendix 1

Statutory Code of Practice June 2013

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf