Closed Circuit Television (CCTV) Purpose & Code of Practice

Document Control

Version Number:	2
Applicable To:	All Academies
Committee:	Values all Students / Premises
Approved By Principals in:	October 2017
Review Cycle:	Two yearly
Date of Next Review:	October 2019
Related Policies:	Behaviour & Exclusion Policy Staff Disciplinary Policy Complaints Policy Grievance Procedure Policy

Revisions

Version	Page/Para No.	Description of Change	Approved On

Contents page

1. INTRODUCTION

The purpose of this code of practice is to regulate the management and use of the closed circuit television (CCTV) system at the Academy.

This CCTV code of practice is operated within Surveillance Camera Code of Practice 2013 published by the Home Office.

This code of practice will be subject to annual review, which will include a review in respect of the effectiveness and necessity of the system.

The CCTV system is a digital system which is owned wholly by the school and is an entirely closed system with no wireless capability. The system does not make audio recordings.

2. OBJECTIVES OF THE CCTV SCHEME

Along with a range of measures, the CCTV system will be used to:

- Help maintain an environment for students, staff and others, which supports their safety and welfare
- Deter crime against persons, and against the school buildings and school assets
- Assist in the identification and prosecution of persons having committed an offence

3. STATEMENT OF INTENT

The CCTV Scheme will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice, as well as the Surveillance Camera Code of Practice 2013 published by the Home Office.

The school will treat as data all CCTV recordings and relevant information. Cameras will be used to monitor activities within the school and grounds in line with the objectives of the scheme. Static cameras are set as to not focus on private homes, gardens and other areas of private property.

Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained in writing for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Materials or knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purpose, or for the purpose of entertainment. Recordings will only be released under the written authority from the Police, or in respect of a subject access request.

The planning and design has endeavoured to ensure that the scheme will give maximum effectiveness and efficiency. It is not possible, however, 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 have been placed at all access routes to areas covered by the school's CCTV.

4. OPERATION OF THE SYSTEM

The system will be administered by the IT Network Manager and senior leadership staff, in accordance with the principles and objectives expressed in the code.

The CCTV system will be in operation 24 hours each day, for every day of the year.

The IT Network Manager will check on a weekly basis that the system is operating effectively and in particular that the equipment is properly recording and that cameras are functional. The

system will be regularly serviced and maintained. Defects will be reported to the servicing company at the earliest convenient opportunity.

5. CONTROL OF SOFTWARE & ACCESS TO THE SYSTEM

Access to the CCTV software will be strictly limited to authorised operators. The main control facility will be kept secure.

Unless in an immediate response to events, staff using the CCTV software must not direct cameras at an individual or a specific group.

Operators must satisfy themselves that all persons viewing CCTV material will have a right to do so.

Other administrative functions will include controlling and maintaining downloaded digital materials, and maintenance and system access logs.

6 MONITORING PROCEDURES

Camera surveillance may be maintained at all times.

Access to monitors is restricted to staff with access to the software system via their PC/laptop and will be used where those areas being monitored are not in plain view.

If covert surveillance is planned or has taken place, copies of the Authorisation Forms, including any Review must be completed and retained.

7. DIGITAL IMAGES: PROCEDURES

Live and recorded materials may be viewed by authorised operators in investigating an incident and recorded material may be downloaded from the system in line with the objectives of the scheme.

Images (stills and footage) may be viewed by the Police for the detection of crime.

A record will be maintained of the release of images to the Police or other authorised applicants. A register will be available for this purpose

Viewing of images by the Police must be recorded in writing and in the log book. Requests by the Police are allowable under section 29 of the Data Protection Act (DPA) 1998

Should images be required as evidence, a digital copy may be released to the Police. The school retains the right to refuse permission for the Police to pass the images to any other person.

The Police may require the school to retain images for possible use as evidence in the future. Such images will be securely stored until they are needed by the Police

Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Principal. In these circumstances, images will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee may be charged at £10 in such circumstances, which is appropriate for subject access requests.
Retention: Images will be retained for only as long as these are required. The system will automatically delete all recordings held on the main control unit after approximately 60 days.

8. BREACHES OF THE CODE (including breaches of security)

Any breach of the CCTV Code of Practice by school staff will be investigated by the Principal, in order for him/her to take any appropriate disciplinary action

9. ASSESSMENT OF THE SCHEME AND CODE OF PRACTICE

Performance monitoring, including random operating checks, may be carried out by the IT Network Manager

10. COMPLAINTS

Any complaints about the school's CCTV system should be addressed to the Principal

11. SUBJECT ACCESS AND FREEDOM OF INFORMATION

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV

Requests for Data Subject Access should be made in writing to the Principal

A request for Subject Access will be charged at £10, which is the maximum allowable under the DPA

A request under the Freedom of Information Act 2000 will be accepted, when such a request is appropriate. Copies of this CCTV Code of Practice (appendix A) will be available on the school's website, or on request from the School reception.

Appendix A: CCTV Code of Practice

1. Introduction and Accountability

The Academy has a comprehensive closed circuit television (CCTV) surveillance system (the system) for the purpose of the prevention and detection of crime and the promotion of health, safety and welfare of staff, students and visitors.

The system is owned by the Academy and images from the system are strictly controlled and monitored by authorised personnel.

This code of practice has been prepared from the standards set out in the Information Commissioner's CCTV Code of Practice 2008 and the Surveillance Camera Code of Practice 2013 published by the Home Office. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the Academy and to ensure that its operation is consistent with the obligations on the Academy imposed by the Data Protection Act 1998. The Code of Practice is widely available consultation from the Academy's website.
In line with the Home Office 12 point code of conduct the use of the system will:

- always be for the purpose specified which is in pursuit of a legitimate aim and necessary to meet an identified pressing need
- take into account its effect on individuals and their privacy
- have as much transparency as possible, including a published contact point for access to information and complaints
- have clear responsibility and accountability for all surveillance activities including images and information collected, held and used
- have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them
- have no more images and information stored than that which is strictly required
- restrict access to retained images and information with clear rules on who can gain access
- consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards
- be subject to appropriate security measures to safeguard against unauthorised access and use
- have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with
- 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, when used in pursuit of a legitimate aim
- be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes

The primary purpose of the system is to:

- help maintain an environment for students, staff and others, which supports their safety and welfare
- deter crime against persons, and against the school buildings and school assets
- assist in the identification and prosecution of persons having committed an offence

2. Operation

The IT Network Manager is responsible for the operation of the CCTV system and for ensuring compliance with this code of practice. Breaches of the code of practice by staff monitoring the system may constitute matters of discipline under the relevant conditions of employment, but it is also recognised that other members of the Academy may have concerns or complaints in respect of the operation of the system.

Any concerns in respect of the system's use or regarding compliance with this code of practice should be addressed to the Principal.

3. System

This code of conduct applies to the Academy site. It will also encompass all other CCTV images that, in due course, are added to the system.

The system is operational and images are capable of being monitored for 24 hours a day throughout the whole year.

Visitors and the general public are made aware of the presence of the system and its ownership by appropriate signage and the publication of this code of practice on the Academy's website. The Academy is responsible for the management and processing of images.

To ensure privacy, wherever practicable the cameras are prevented from focusing or dwelling on domestic accommodation and this will be demonstrated on request to local residents. Where it is not practicable to prevent the cameras from focusing or dwelling on such areas or where domestic property is adjoining the school site, appropriate training will be given to the system operators to ensure that they are made aware that they should not be monitoring such areas.

Images captured on camera will be recorded on the main CCTV servers which are held in a secure location. Although every effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

For the purposes of the Data Protection Act 1998, the Data Controller is the Academy and the Academy is legally responsible for the management and maintenance of the CCTV system.
No unauthorised access to the system is allowed at any time. Normal access is strictly limited to authorised staff only. Police officers may view recorded material with the consent of the Director of Services.

Persons other than those specified may be authorised to access the CCTV material on a case-by-case basis. Written authorisation is required. Each separate visit will require individual authorisation and will be supervised at all times. Such visitors will not be given access to any data which falls within the scope of the Act.

In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to access the CCTV system.

Before granting access to the CCTV system, controllers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors log, which shall include their name, department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the start and finish times of their access to the CCTV system.

It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the procedures. The Director of Services will be responsible for the development of, and compliance with, the working procedures of the system.

Recorded images will only be reviewed with the authority of the Principal/Vice Principal. Copies of digital images will only be made for the purposes of crime detection, evidence in

relation to matters affecting safety, evidence for prosecutions, or where otherwise required by law.

All staff involved in the operation of the CCTV system will, by training and access to this code of practice, be made aware of the sensitivity of handling CCTV images and recordings.

The It Network Manager will ensure that all staff, including relief staff, are fully briefed and trained in respect of all functions; operational and administrative, arising within the CCTV control operation. Training in the requirements of the Data Protection Act and this code of practice will also be provided.

4. Recordings

The system is supported by digital recording facilities which will function throughout operations in real time.

As the images are recorded digitally, the process of identifying retrieval dates and times will be computerised. Images will be cleared automatically after a set time.

Unless required for evidential purposes or the investigation of crime, recorded images will be retained for no longer than 60 days from the date of recording. However, the Academy recognises that, in accordance with the requirements of the Data Protection Act, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images. Digital images will be automatically erased after a set period, which will be no longer than 60 days.

In the event of the digitally recorded image being required for evidence or the investigation of crime it will be retained for a period of time until it is no longer required for evidential purposes or any investigation into a crime has been completed.

5. Digital Recording and Access Procedures

All disks containing images to and remain the property of the Academy. Disk handling procedures are in place to ensure the integrity of the image information held.

Requests by persons outside the Academy for viewing or copying of disks or obtaining digital recordings will be assessed on a case by case basis.

Requests from the police will arise in a number of ways, including:

- requests for a review of recordings in order to trace incidents that have been reported
- immediate action relating to live incidents, eg immediate pursuit
- for major incidents that occur when images may have been recorded continuously
- individual police officers seeking to review recorded images on screen

Requests for access to recorded images from persons other than the police or the data subject (that is, the person whose image has been captured by the CCTV system) will be considered on a case by case basis. Access to recorded images in these circumstances will only be granted where it is consistent with the obligations placed on the Academy by the Data Protection Act 1998 (DPA) and, in particular, with the purposes set out in Section 1 of the DPA.

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose

copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the code of practice reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998.

All staff should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

Access to recorded images will be restricted to staff who need to have access in order to achieve the purposes of using the equipment.

All access to the disks on which the images are recorded will be documented.

Disclosure of the recorded images to third parties will be made only in the following limited and prescribed circumstances and to the extent required or permitted by law:

- law enforcement agencies where the images recorded would assist in a specific criminal inquiry
- prosecution agencies
- relevant legal representatives
- people whose images have been recorded and retained and disclosure is required by virtue of the Data Protection Act 1998

All requests for access or disclosure will be recorded. The Principal will make decisions on access to recorded images by persons other than police officers. Requests by the police for access to images will not normally be denied and can be made without the above authority, provided they are accompanied by a written request signed by a police officer who must indicate that the images are required for the purposes of a specific crime enquiry.

If access or disclosure is denied, the reasons will be documented. If access to or disclosure of the images is allowed then the following will be documented:

- the date and time at which access was allowed or the date on which disclosure was made
- the reason for allowing access or disclosure
- the extent of the information to which access was allowed or which was disclosed

Appropriate forms will be used to document routine disclosure to the Police.
Requests for non-Police disclosures will be forwarded to the Principal.
All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of data subject access requests.

Data subjects will be asked to put in writing any requests for access. Individuals should provide:

- dates and times when they visited the Academy and their location; for example which specific area or building
- either a cheque or cash to the sum of £10.00 for which a receipt will be issued.

The data subject will be asked whether they would be satisfied with merely viewing the images recorded.

A written decision on their request will be sent to the data subject within 21 days and, if access to the images is to be provided (see below for circumstances when it may be refused), such access will be provided within 40 days of the Academy receiving the request or, if later, the date when the Academy receives the identification evidence from the data subject.

The procedure outlined above and the use of the subject access request form complies with Section 7 of the Data Protection Act 1998, enabling the Principal to inform individuals as to whether or not images have been processed by the CCTV system. The Academy is not obliged to comply with a request under this section unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the information which that person seeks.

Where the Academy cannot comply with the request without disclosing information relating to another individual who can be identified from that information it is not obliged to comply with the request, unless:

- the other individual has consented to the disclosure of the information to the person making the request, or
- it is reasonable in all the circumstances, including having consideration to child protection, to comply with the request without the consent of the other individual

6. Photographs and hard copy prints

Photographs and hard copy prints taken from digital images are subject to the same controls and principles of Data Protection as other data collected. They will be treated in the same way as digital images.

At the end of their useful life all computer disks, still photographs and hard copy prints will be disposed of as confidential waste.

This code of practice will be reviewed annually to assess its implementation and effectiveness and it will be promoted and implemented throughout the Academy.

Appendix B: Record of a request to review CCTV images at _____

Name of the person making the request to check CCTV cameras			
Date of incident			
Time of incident			
Area of school to review			
Reason for request (outline the incident that you would like the cameras checking for)			
Name of the person reviewing the recordings			
In the presence of			
Action taken by reviewer	No incident identified	✓	×
	Incident found & incident confirmed by (name)		
	Incident found & images copied to disc	✓	×
	Disc number		
	Disc handed to		
	Date that disc was returned to IT support and stored		
Action taken by IT support with disc	Stored	✓	×
	Date destroyed/deleted		

Signed _____