



Kingsthorpe College

A Designated Specialist Sports College



CCTV Protocol and Policy

For

PFI and KC CCTV SYSTEMS at Kingsthorpe College

Date of Adoption:	19 th January 2009
Frequency of Review:	Annually
Review Date due:	January 2010
File Name:	CCTV Policy
Policy Number:	2 Z

Contents

1.0	Introduction and Objectives	2
2.0	System Administration	2
3.0	CCTV System Operations	3
4.0	Security Procedures for CCTV R&PF and Viewing Areas.....	4
5.0	Incident Reporting	4
6.0	Complaints Procedure	4
7.0	Observed Occurrence and Incident Action Documentation.....	4
8.0	Management of and Access to Recorded Material.....	4
9.0	Subject Access Request.....	5
10.0	Police and Criminal Evidence Act 1984 (PACE)	6
10.1	Declaration of Confidentiality.....	6
11.0	Fault Reporting Procedure	6

1.0 Introduction and Objectives

This CCTV protocol has been compiled to document the day to day procedures required to provide an effective and compliant operating system for CCTV Systems installed at Kingsthorpe College.

There are two CCTV systems installed at Kingsthorpe College

System 1:- Consists of 5 external and 1 internal (Reception) cameras installed as part of the PFI building project hereafter referred to as PFI CCTV

System 2:- Consists of 7 external and 60 internal CCTV cameras installed by Kingsthorpe College in August 2008, hereafter referred to as KC CCTV

By complying with the contents of this protocol, an audit trail sufficient to satisfy the legal requirements of the Data Protection Act, the Police and Criminal Evidence Act and other relevant legislation will be maintained, ensuring that data security, evidence admissibility and civil liberties are not compromised.

2.0 System Administration

Responsibility for the operation and administration of the CCTV system will be shared by the Data Controller, System Managers (both KC and Amey) and System Operators.

The Data Controller

The Data Controller at Kingsthorpe College is the Principal who takes ultimate responsibility for determining the purposes for and the manner in which data is processed, and for ensuring that processes are in place to prevent unauthorised disclosure of captured data. However the day to day processes are delegated to the Director of Administration.

The responsibilities of the Data Controller include:

1. Defining the purpose of the CCTV Installation:

CCTV is installed at Kingsthorpe College to:

- Prevent and detect crime
- Apprehend and prosecute offenders
- Assist in the management of pupil behaviour
- Support Health & Safety objectives where appropriate

2. Informing others of the purpose of the CCTV Installation –

Signage will be displayed at entrances to the College

Parents will be notified as to the purpose of the CCTV installation at Kingsthorpe College annually through the College newsletter.

3. Deciding how long CCTV data will be retained –

The digital hard drives installed at the College on both the PFI and KC systems will be set to automatically erase data captured after seven days. In the case of CCTV footage of any incidents that require investigation the data will be downloaded to a secure area of the College network and retained until investigations are completed. It will then be erased.

4. Controlling access to data –

Given the nature of CCTV data, it is highly likely that 'personal data' (images of persons) and possibly 'sensitive personal data' (e.g. persons committing crimes). The Data controller will therefore be responsible for ensuring that access to, and disclosure of, recorded images is restricted and carefully controlled.

To this purpose data access will be limited to the following Data Operators:

- The College Leadership Team
- Directors of Houses and House Managers
- IT Network Manager and IT Technicians
- Amey SFO (in the case of the PFI CCTV only)

The System Managers

PFI CCTV - Acting under the control of the Data Controller, the PFI System Manager (Northampton Schools Ltd, delegated to Amey FM) will be responsible for the management and maintenance of the physical system. He will ensure that best practice is adhered to, that records are auditable and that data is made available in accordance with legal requirements.

KC CCTV - Acting under the control of the Data Controller, the KC System Manager will be the Kingsthorpe College IT Network Manager who be responsible for the management and maintenance of the physical system. He will ensure that best practice is adhered to, that records are auditable and that data is made available in accordance with legal requirements

The System Operators

The system operators have day to day access to and control of the system and will carry out the procedures laid down in this protocol. They must comply with instructions from the Data Controller or System Manager to ensure that the data under their control is not compromised. These persons will be formally appointed and aware of their obligations and responsibilities. Access to the CCTV data will be by means of password protection.

The System Operators are:

- The College Leadership Team
- Directors of Houses and House Managers
- IT Network Manager and IT Technicians
- Amey SFO (in the case of the PFI CCTV only)

3.0 CCTV System Operations

The majority of the day to day operation of the system will require a good deal of input from the System Operators (In the case of PFI CCTV reporting to the FM Contractor). Suitable regular checks should be in place to ensure that:

1. All cameras are functioning correctly.
2. Camera views are correct and do not infringe upon inappropriate areas.
3. All multiplexing, recording and monitoring equipment is operational and properly set.
4. Tapes, disks or other recording material are properly inserted and functioning.
5. Used tapes, disks or other recorded media are passed to the Data Controller to be securely stored.
6. All documentation handed over is complete and up to date.
7. Systems are not left 'logged in' while Operators are not in attendance.

A System Log Book will be located in the Director of Administration's office, all Operators should maintain a written log of access and activity.

Note: The Operators must at all times be aware that they have access to restricted data and that they must not communicate any information to persons other than the system Owner, Manager, Data Controller or persons authorised by them.

It is also important to note that the service requirements of the PFI Contract do not require Amey to monitor the data being captured during the required operating period.

4.0 Security Procedures for CCTV Systems

Access to the CCTV Equipment should be restricted at all times to prevent unauthorised access to data. This will be achieved through the use of password protection. The Data Controller will ensure that passwords are changed termly.

5.0 Incident Reporting

When an incident occurs, the Operator, Manager or Controller should:

1. Operate camera and screen controls to ensure that the appropriate footage has recorded, having due regard for the privacy of individuals not committing an offence.
2. Along with the maintenance of the Log Book, fill out 'CCTV Incident report Form'. This must be carried out immediately after or as soon as possible after the reported incident.
3. Inform the System Manager and Data Controller of the incident at the earliest opportunity and comply with any instructions received.

6.0 Complaints Procedure

Upon receipt of a complaint regarding captured data the Controller or Manager should:

1. Record the date and time of the complaint
2. Fill in relevant sections of the CCTV Complaints Form'. The complainant should be asked for their preferred method of communication and wherever possible this method should be utilised.
3. Pass a copy of form to the System Manager or Data Controller.

Upon receipt of the form from the Data Controller will:

1. Instigate an investigation, either personally or by delegation to an appropriate investigator.
2. Fill in relevant sections of the form as appropriate and notify the complainant of the result of the investigation.
3. Should the complainant wish to appeal against the investigators decision, complete 'Appeals Procedure Form' and appoint a different investigator.

(Upon completion of the appeals investigation the appellant will be notified of the result).

7.0 Observed Occurrence and Incident Action Documentation

When an Operator observes an incident in the course of his/her normal duties, the actions prescribed in the "Incident Report" section will be carried out, including the logging of all relevant information and completion of relevant forms

8.0 Management of and Access to Recorded Material

Recorded material will be stored on the hard drive of the CCTV Equipment, and also possibly on external tapes, disks or drives in line with the Data Controllers procedures.

Data that is downloaded from the system which contains footage of an incident that needs to be stored for future review or to be used as evidence, will be carried out in accordance with the following procedures.

- The data will be downloaded in to a secure folder on the College IT network. Only the Data Controller, the System Manager will have access to this area.
- Recorded data will be deleted as soon as the incident has been investigated and resolved. If no resolution is reached the data will be deleted after 30 days unless the incident is still part of an ongoing investigation.

Where the Police are involved in this process a data disclosure form must be completed. And data taken from the system should be locked in a separate and suitably secure container. When any tape/disk is removed from the secure storage for review, disclosure to Police or other body, or viewing by a subject granted access by the Data Controller, records of all access and all person accessing this data should be carefully maintained.

Access to recorded material will be restricted to the System Managers and the System Operators under instruction from the Data Controller. Recorded information will only be accessible from:

PFI CCTV – The stand alone system located in the Reception Office

KC CCTV – The CCTV PC located in the Reception Office, the server and the PC's of the IT Network Manager and Director of Administration

9.0 Subject Access Request

When a person makes a request to view any data held on recorded media and pertaining to them, they should be referred to the System Manager or Data Controller.

Requests for personal data by official bodies, such as Police, Inland Revenue or Customs and Excise, must be made on an official access request form.

The Data Controller, having satisfied himself/herself of the subjects identity, will review the material requested (complying with all procedures previously mentioned in this manual) and will decide whether access can be granted. A written response to the data subject must be made within 40 days.

If the Subject Access Request is granted it may be possible to provide a copy to the subject, otherwise viewing in a controlled environment should be arranged.

Note: Subject access rights are governed by data protection legislation and include the following provisions:

- a) a fee is paid for each search
- b) a person gives sufficient and accurate information about a time and place
- c) the Data Controller/Manager only shows information relevant to that search

If a request is made for a copy, then only data pertaining to that person is copied. A search request should provide sufficient information to locate the data requested (e.g. it could be specified in 30min slots for a given date and place). If insufficient or inaccurate information is provided a data controller may refuse the request until sufficient information is provided.

If it is decided that the Data Request cannot be granted, the subject must be notified in writing, stating the reason why (e.g. the data is to be used in legal proceedings).

Blurring of Images on Disclosure

When reviewing material to assess its suitability for disclosure, the footage requested might contain images of other persons whose civil liberties might be compromised. In this case permission must be sought from them before disclosure can be granted to the applicant.

If it is impossible for permission to be obtained and there is no other reason to deny access to the applicant, then the footage requested must be edited to blur the images of other subjects in order to protect their interests.

10.0 Police and Criminal Evidence Act 1984 (PACE)

Section 78(1) of PACE Act 1984 deals with the use of recorded data to identify suspects and the circumstances under which record images may be inadmissible.

The Act applies, in the main, to Police procedures therefore they will advise as to actions required by the administrators of the CCTV system, when a criminal investigation is undertaken.

10.1 Declaration of Confidentiality

It is necessary for all persons involved in the control and administration of the CCTV system to sign a declaration of confidentiality in which they agree to abide by the Code of Practice and Operating Manual associated with the system.

Managers, Operators and third parties must complete a Declaration of Confidentiality, before they are permitted to have any form of contact with the CCTV system.

11.0 Fault Reporting Procedure

PFI CCTV - All faults that manifest themselves on any PFI CCTV equipment or any of the associated equipment located elsewhere, including cameras, should be reported to the Amey System Manager (by raising an event on the Helpdesk)

The System Manager (Amey) will make arrangements for suitably qualified contractors to carry out necessary repairs. Any works which might potentially enable such contractors to access controlled data, should be supervised by the System Manager or Data Controller.

KC CCTV - All faults that manifest themselves on any KC CCTV equipment or any of the associated equipment located elsewhere, including cameras, should be reported to the KC System Manager.

The KC System Manager will make arrangements for suitably qualified contractors to carry out necessary repairs. Any works which might potentially enable such contractors to access controlled data, should be supervised by the System Manager or Data Controller

In both cases any works which might potentially enable such contractors to access controlled data, should be supervised by the System Manager or Data Controller. All works carried out should be recorded in the System Log Book.