



CCTV Code of Practice

Version:	3.0
Date reviewed:	March 2022
Review date:	May 2024
Approved by Governors:	May 2022

Key authorising signatories to the PFI Project CCTV code of practice.

School Representative..... Date ..30-01-20.....

NameSteve Walsh.....

Job Title.....School Business Manager.....

QED.....Date

Name Job Title.....

Pinnacle FM Date

Name Job Title.....

Contents

	Page
Introduction	3
Disclosure	4
Operation and maintenance	5
Access	5
Communication	7
Additional Information	7
Appendix A - Data Protection Principles	9
Appendix B - The guiding principles of the Surveillance Camera Code of Practice	10
Appendix C - Expansion of requirements	11
Appendix D - Operational Compliance Guidance	12

Appendix E - CCTV System Authorised Users	14
Appendix F - Right of Access Form	15
Appendix G - Maintenance Log	17
Appendix H - Incident, view & disclosure log	18

Data Controller A person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor Any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller.

1. INTRODUCTION

Closed Circuit Television (CCTV) is a method of observing places and people, usually from a distance. It comprises of one or more cameras viewing a 'scene' and displaying that scene to a CCTV operator on a monitor screen. The images viewed may be recorded for later playback. This Code of Practice is concerned only with recorded images that can be retrieved on demand at a later date.

CCTV surveillance is an increasing feature of our daily lives and could intrude into our private lives. Therefore, for public confidence and to meet legislative requirements the schools CCTV system needs to be managed.

This document sets out the accepted use and management of the CCTV system and images to ensure the compliance with the General Data Protection Regulation (GDPR) and associated legislation ('data privacy legislation'), the Human Rights Act 1998 (HRA), the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA Code) and other legislation.

Where images are 'real time' and not recorded then Data Protection Legislation does not apply, but other legislation or policies may.

This document relates only to CCTV systems that is operated within the PFI Fairfield School Contract.

It does not cover –

- Targeted and Intrusive Surveillance Activities which are covered by the Regulation of Investigatory Powers Act (RIPA).
- Use of surveillance techniques to monitor employees' compliance with their contracts of employment if any such surveillance exists.
- Use of cameras and similar equipment by the media for the purposes of journalism, or for artistic or literary purposes.

- 1.1 The purpose of the Closed Circuit television (CCTV) operating on the Fairfield School PFI contract is to aid in the protection of the school's premises. The system will be used as a deterrent or to record acts of damage or criminal offence.
- 1.2 The System installed as part of the building works at Fairfield School will cover the staff car parking area and main entrance to the school. Locations have been drawn up in consultation with Kirklees Council (KC), the SPV, and Fairfield School and has been subject to review with "Secured by Design". CCTV signs are located at the main school entry point. The operating system is the property of SPV while all rights in the material recorded using the CCTV equipment (including any copies of such material or images extracted from it) shall automatically vest in and remain the property of the school. PINNACLE FM will undertake the day to day operation of the system.
- 1.3 Fairfield School will be considered the Data Controller and as such have a duty to comply with the principles as set out in Data Protection Legislation. PINNACLE FM will be considered Data Processor and as such have a duty to comply with the data protection principles set out in Data Protection Legislation. The Parties have considered the appropriate legislation and considers the CCTV System compliant, meeting the requirements as prescribed by Data Protection Legislation.

The CCTV scheme has been registered with the Information Commissioner under the terms of the Data Protection Act 2018 and General Data Protection Regulation and will seek to comply with the requirements of the Commissioners CCTV Code of Practice.

1.4 The purpose of the System is to:

- 1.4.1 Protect the school premises by acting as a deterrent against acts of damage or criminal offence;
- 1.4.2 Protect the school premises by recording acts of damage or criminal offence.

However, the Data Controllers will allow the system to be used (to be reviewed on an annual basis):

- 1.4.3 By the school authorities to view instances where issues relating to student safety have been captured and recorded by the cameras used for the protection of the school premises;
- 1.4.4 By the school authorities to view instances where property damage or criminal activity has been recorded;
- 1.4.5 By the police to view or make copies where criminal activity has been recorded.

2. DISCLOSURE

2.1 In order to comply with current Data Protection Legislation, there are only limited circumstances where the Data Controllers are entitled to disclose "personal data" which is recorded by the system. Disclosure in this sense would include permitting the viewing of screens in the Superintendent's office, permitting the viewing or removing of tapes or photographs, or giving the Police or other individuals or organisations information about

recorded personal data. The Data Controllers are entitled to disclose personal data in any of these ways if:

2.1.1 The purposes of the disclosure are consistent with the Data Controllers notification to the Information Commissioner, and

2.1.2 The purposes of the disclosure fall within the objectives of 1.4.1 to 1.4.5 above (i.e if the purpose is the protection of the premises, protection of the students or detection and prosecution of crime), and if the Data Controllers have confirmation from the person seeking disclosure that the failure to disclose would prejudice those purposes, and

2.1.3 The disclosure is required under a special statutory power or rule of law, or if a court orders disclosure.

2.1.4 In addition to this, the Data Controllers will comply with the Human Rights Act 1998.

2.2 Fairfield School CCTV system will be managed on a day-to-day basis by PINNACLE FM. As managers on behalf of the school, PINNACLE FM will be considered Data Processor and will comply with the principles pursuant to Article 5 of the General Data Protection Regulation which requires that:

2.2.1 "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

2.2.2 PINNACLE FM will ensure compliance in the following ways;

2.2.3 Adherence by PINNACLE FM and its staff to Fairfield School CCTV Code of Practice

2.2.4 Adherence by the Third Party Security Contractors to Fairfield School CCTV Code of Practice

2.2.5 Appropriate training of PINNACLE FM staff and Third Party Contractor staff in the application of the Fairfield School CCTV Code of Practice

3. OPERATION & MAINTENAINCE

3.1 The CCTV systems will be installed and administered by Pinnacle FM

3.2 Pinnacle FM will ensure checks to the system and will confirm the efficiency of the CCTV system and in particular that the equipment is properly recording and that cameras are functional.

3.3 Pinnacle FM will be responsible for maintaining system maintenance logs.

3.4 CCTV systems shall not be used for general surveillance of staff or visitors or for purposes not compatible with the purposes indicated above.

- 3.5 Where law enforcement organisations request control of the system (e.g. to mount a specific surveillance operation) then the CCTV Manager (Head teacher of School) will ensure that she/he is satisfied as to the legality of the request and that appropriate documentation and controls are in force to maintain the basic operational principles of CCTV usage.
- 3.6 The CCTV system as no audio recording function should this change the policy should be reviewed.
- 3.7 The schools listed within this code of practice are considered to be Data Controller's in accordance with the principles and objectives expressed in the ICO Code of Practice.
- 3.8 Day to Day operational management of the CCTV systems is delegated to Pinnacle FM
- 3.9 CCTV systems throughout the schools listed will be operational, but not manned 24 hours each day, every day of the year.
- 3.10 Disks, electronic images and any recording format containing images belong to, and remain the property of, the school.
- 3.11 CCTV systems will automatically overwrite recordings and delete on a loop system every 30 days
- 3.12 Other administration functions will include maintaining the accuracy of time clocks, service records and that recorded images are overwritten after a period of 30 days

4. ACCESS

- 4.1 Under the GDPR and DPA 2018, individuals have the right to obtain information held about them.
- 4.2 Data Subject Access Request should be made to the Head teacher of Fairfield School
- 4.3 The school will verify the identity of the person making an application for information before any information is supplied.
- 4.4 Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Head teacher of School
- 4.5 Disks containing images belong to, and remain the property of Fairfield School
- 4.6 All requests will be responded to without delay and at the latest, within one month of receipt.
- 4.7 In the event of numerous or complex requests, the period of compliance will be extended by a further two months as prescribed by the ICO. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

- 4.8 The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should be reasonably specific, for example, specified to the nearest half-hour
- 4.9 Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law;
- 4.8.1 The police – where the images recorded would assist in a specific criminal inquiry
- 4.8.2 Prosecution agencies – such as the Crown Prosecution Service (CPS)
- 4.8.3 Relevant legal representatives – such as lawyers, barristers and solicitors.
- 4.8.4 Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation.
- 4.9 Final decisions on disclosure and the release of information are to be made by the Head Teacher of Fairfield School
- 4.10 Contractors (relating directly to the CCTV system). All contractor visits will be by arrangement. All contractors will be instructed to report to the Superintendent in the first instance. The Superintendent must be satisfied of the identity and purpose of the visit before allowing access to the recording and monitoring equipment.
- 4.11 A record book will be kept of all visitors who request access to the System whether it be to use the monitoring equipment, view recorded images, to remove downloaded images or to maintain the System. Visitors will be requested to complete the book recording details of individual, organisation and time of arrival and departure and reasons for requiring access to the System. (This will be recorded via the Helpdesk, contact details are as follows; Kirklees.Helpdesk@pinnaclepsg.co.uk or Telephone 0800 0327567)
- 4.12 An evidence log must be maintained to record movement of downloaded images from the Superintendent's office. . (This will be recorded via the Helpdesk, contact details are as follows; Kirklees.Helpdesk@pinnaclepsg.co.uk or Telephone 0800 0327567)
- 4.13 A photograph register will be maintained to record the printing of photographs from the system and their removal from the school premises. . (This will be recorded via the Helpdesk, contact details are as follows; Kirklees.Helpdesk@pinnaclepsg.co.uk or Telephone 0800 0327567)
- 4.14 The system installed at Fairfield School does not have this facility, however, should the system require modification to enable such photographs to be taken from recorded images, this paragraph will be applicable.
- 4.15 Police viewing of images will be by prior arrangement with PINNACLE FM. In exceptional circumstances immediate viewing of images may be required by the Police. A record will be maintained in the visitor book of any such visits. Police must complete an access request form.

4.16 Other duties may be designated to Caretakers, including liaison with emergency services and third party security firm as referred to in paragraphs 5.2 to 5.4 below.

5. COMMUNICATION

5.1 The emergency procedures set out in the PINNACLE FM Contract Management Plan will be used in appropriate cases to call the Fire Brigade, Ambulance Services and police.

5.2 In addition, liaison with other units is necessary.

5.3 Details are available within the PINNACLE FM Contract Management Plan of points of contact with the following, and are continuously updated:

5.3.1 Fire & Rescue Service

5.3.2 Ambulance Service

5.3.3 Police

5.3.4 School Contact

5.3.5 PINNACLE FM Contract Staff

5.3.6 PINNACLE FM Helpdesk

5.3.7 SPV – (QED)

5.3.8 Kirklees Council

5.3.9 Third Party Security Contractors and CCTV Maintenance contractors

5.3.10 Others as necessary

6. ADDITIONAL INFORMATION

6.1 Breaches of the code (including breaches of security). Any breach of the Code of Practice by school staff will be initially investigated by the Head teacher of Fairfield School, in order to take the appropriate disciplinary action. Complaints will be dealt with in accordance with the ICO Code of Practice.

6.2 Breaches of this Code of Practice by staff may lead to disciplinary action being taken which could result in dismissal and staff may be subject to possible criminal proceedings.

6.3 Images will only be used by the Data Controller for internal disciplinary action where it is permitted to do so under current Data Protection Legislation and the Human Rights Act 1998

- 6.4 Any complaints concerning the school's CCTV system within this code of practice should be addressed to PINNACLE FM. Complaints will be investigated in accordance with the Contract Management plan.
- 6.5 Retention periods need to be suitable for the purpose and images should not be kept any longer than considered necessary. It is imperative that access to, and security of the images is managed in accordance with the requirements of the DPA and the CCTV Code. At all times the following standards are to be applied:
- 6.6 CCTV images not to be retained for longer than necessary. Data storage is automatically managed by the CCTV digital records which use software programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces an approximate 30-day rotation in data retention.
- 6.7 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal proceedings), the images will be erased following the expiration of the retention period.
- 6.8 If CCTV images are retained beyond the retention period, they are to be stored in a secure place to which access is controlled and are to be erased when no longer required.
- 6.9 CCTV systems must not be used for general surveillance of staff or visitors or for purposes not compatible with the purposes indicated above.
- 6.10 Where law enforcement organisations request control of the system (e.g. to mount a specific surveillance operation) then the CCTV Manager (Head teacher) (or equivalent) will ensure that she/he is satisfied as to the legality of the request and that appropriate documentation and controls are in force to maintain the basic operational principles of CCTV usage.
- 6.11 Liaison meetings may be held with the Police and other bodies.
- 6.12 Recording discs used will be properly indexed, stored and destroyed after appropriate use.
- 6.13 Discs may only be viewed by Authorised School Officers and the Police.
- 6.14 Discs required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- 6.15 Discs will not be made available to the media for commercial or entertainment.
- 6.16 Discs will be disposed of securely by incineration.
- 6.17 Additional information and guidance can be found on the ICO website: - <https://ico.org.uk/>
- 6.18 CCTV Code of Practice:- <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Appendix A

Data Protection Principles

- 1) processed lawfully (Article 6, 9), fairly and in a transparent manner in relation to individuals;
- 2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- 6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 7) The Data controller shall be responsible for and be able to demonstrate, compliance with the above six principles

Appendix B - The guiding principles of the Surveillance Camera Code of Practice

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then 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.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Expansion on the requirements of the Data Protection Act & General Data Protection Act

		Yes/No/ Comments
1.	Do all system users have an awareness of: -? <ul style="list-style-type: none"> • Preventing processing likely to cause substantial or unwarranted damage to an individual. • Preventing automated decision taking in relation to an individual. 	
2.	Is the person responsible for responding to SAR'S clearly identifiable to system users/operators	
3.	In relation to a request to prevent processing (individual's right to request) is there a response process which clearly states whether or not the request will be complied with, and if not to be complied with states the reason(s)?	
4.	Is there a procedure to ensure that a written response to a (3.) request, stating the decision, must be sent within 21 days of receipt of the request? A copy of the response should be retained.	
5.	Is there a procedure to document: -? <ul style="list-style-type: none"> • The original decision • The request from the individual • The response to the individual. 	

Appendix C

The Quality of images must be fit for the system purpose failure to produce adequate images for the stated purpose of the system breaches the Data Protection Act.		
		Yes/No/ Comments
1.	Upon installation does the system perform properly?	
2.	Is all equipment sited in such a way that it only monitors those areas that are intended to be covered by the equipment and or have measures to prevent images being captured within neighbouring sites?	
3.	Are cameras protected where necessary e.g. from vandalism - by being boxed in, out of reach.	
4.	If the system records location/date/time is this information accurate?	
5.	Can the system be searched using records location/date/time?	
5.	Are system operation instructions available for operators?	
6.	Does a regular maintenance/service schedule of the system exist to ensure clarity of pictures is a maintenance log kept?	
7.	Are adjustable cameras restricted to prevent surveillance of areas not designated for such?	
8.	<p>Is signage (for overt surveillance) clearly visible?</p> <p>The signs must -</p> <ul style="list-style-type: none"> • Identify the responsible person and/or organisation [e.g. KC] • The purpose of the scheme [e.g. Prevention and detection of crime] • Details of whom to contact regarding the scheme [e.g. Head of Security XXXXXXXX] • The signs (and wording) must be of an appropriate size. 	
9.	<p>If a camera is damaged is there a clear procedure for: -</p> <ul style="list-style-type: none"> • Defining the person responsible for making arrangements for camera repair. • Ensuring the camera is fixed within a specific time. • Checking the quality of the maintenance work. 	

Appendix D – Operational Compliance Guidance

Operator Training Check List

School and Remote Operators		
		Yes/No/ Comments
1.	Have operators received adequate training relating to reviewing and retrieving images?	
2.	Are operators aware of the purpose of the surveillance (which will guide their actions)?	
3.	Are operators trained in recognising the privacy implications of surveying such areas i.e. implication for neighbours?	
4.	Are operatives aware of: - <ul style="list-style-type: none"> • This policy? • Data Protection Principals listed in this policy? • Their responsibility in relation to: - <ul style="list-style-type: none"> ○ Reporting faults including blurred images to the FM help desk ○ Recording any CCTV Maintenance in the maintenance log records? ○ Subject Access Requests and the policy standard form and how to use it? ○ Log of access ○ Control Room access protocol? 	

Disclosure of images to third parties must be for valid and legal reasons and documented		
		Yes/No/ Comment
1.	Is access to the images restricted to authorised persons?	
2.	Are procedures in place to document any access to image recordings?	
3.	Are disclosure rules documented? Disclosure should only be made in limited and prescribed circumstances e.g. if disclosed for prevention & detection of crime then likely recipients are: The Police, prosecution agencies, legal representatives. Either a data sharing agreement should be in place or each disclosure covered by a Section 29(3) request form.	
4.	Are all requests for access recorded – even if disclosure is not made?	
5.	Where access is allowed is the following recorded- Date and time access allowed or images disclosed Identity of third party allowed viewing or receiving images The reasons for allowing access Extent of the images/information disclosed	
6.	Are images that should <u>not</u> be made widely available documented e.g. those not for disclosure to the media?	
7.	Are reasons for making images widely available documented	
8.	Can images be blurred before disclosure to a media company (requirement). It may be necessary to indent an editing company who can do this	
9.	If an editing company is appointed: - Does a contract exist between the CCTV owner and the company? Has the editing company given guarantees re security measures e.g. their staff vetting procedures, storage of images?	

	<p>The CCTV owner should check that the guarantees are met?</p> <p>Does the contract clearly state that the editing company can only use images in accordance with instructions of the CCTV owner?</p> <p>Does the contract clearly state the security guarantee of the editing company?</p>	
10.	If the media organisation is also the editing company the above will apply?	

Processing of personal images must conform to Data Protection principles		
		Yes/No/ Comments
1.	Does an image retention policy exist - that not only states the length of time images should be retained but encompasses an active schedule for deleting images? Note: any retention policy should be included or referenced in this Code of Practice.	
2.	<p>Where images are retained is the reason for so doing documented? Note: The following must be recorded: -</p> <ul style="list-style-type: none"> • Date of retention decision/action. • The reason for retention. • Any reference number e.g. crime incident number • Location of the images 	
3.	Are retained images stored in a secure place, access to which is controlled?	
4.	Are surveillance monitors only viewable by authorised people?	
5.	Are all access requests controlled by an authorised person or persons?	
6.	Is there an appropriate viewing area where only authorised people can see the images?	
7.	<p>Where images are removed from the system for viewing is there a system for recording: -</p> <ul style="list-style-type: none"> • Date and time of removal. • Name of person removing the images. • Name (and organisation) of any person viewing the images. • The reason for viewing. • The outcome, if any, of the viewing. • Date and time of return of the images to the system or secure place if images are retained further. 	
8.	Do system users know the procedures applicable to accessing recorded images?	
9.	<p>Are procedures in place to train all operators in: -</p> <ul style="list-style-type: none"> • System use responsibilities? • System user's disclosure policy • Rights of individuals in relation to their recorded images. 	

Appendix F – Right of Access Form

Fairfield School Subject Access Request (SAR)

Please complete and return this form to the Head teacher of Fairfield School

Data Protection Act 2018
General Data Protection Regulation
RIGHT OF ACCESS TO PERSONAL DATA: CCTV IMAGES

- Please complete the form as fully as possible.
- You may be asked to supply evidence of your identity e.g. driving licence, passport or utility bills in your name/address.
- If you are asking for footage about someone else you must have written permission from them giving the authority for you to do so.

SECTION 1 – YOUR DETAILS

First name(s)		Last name	
Address			
Post code			
E-mail address			
Telephone no.			

SECTION 2 – DETAILS OF DATA SUBJECT IN CCTV FOOTAGE (if different from above)

First name(s)		Last name	
Address			
Post code			

Please note that if you are not the subject of the CCTV footage you must provide evidence that you have permission to ask for it e.g. a letter of authorisation or Power of Attorney etc. (Please send a copy with this request)

SECTION 3 – AGENCY OR REPRESENTATION DETAILS (Please tick if appropriate and supply documentation of which exemption under the Data Protection Act 2018 you wish to apply)

Do you represent the police and the images are required to prevent/detect a crime?	
Do you represent a prosecution agency and require the images to prosecute an offender?	
Are you a solicitor or barrister and require the images in connection with legal proceedings?	
Do you represent the media, where disclosure of the image to the public is needed in order to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident?	
Any additional information to identify request i.e. crime reference number	

SECTION 4 – DETAILS OF REQUIRED IMAGES (Please provide the following information to assist in the search for CCTV images)

Date image was recorded		Time image was recorded (within 30 mins)	
-------------------------	--	--	--

Location of footage (street, building, other landmark)			
Please provide a description of the incident you wish to view			
Please provide a photograph of yourself (or the subject), or a description, that will enable the operator to identify you/them on the CCTV footage	Photograph provided? (please circle as appropriate)	Yes	
		No	
Do you want to view the footage in person? (please circle as appropriate)	Yes	Do you want a still image from the footage? (please circle as appropriate)	Yes
	No		No

Signature of subject at Section 1.....

Date

Signature of subject at Section 2.....

Date
(if applicable)

IMPORTANT INFORMATION:

Presentation of all original documentation, for example, proof of identity, letter of authorisation, will be required at the point of release of CCTV footage.

Appendix G – Maintenance Log

CCTV Maintenance Log

(Ref to O&M manual for manufactures and installer information)

The equipment should be constantly monitored for effective operation and any problems reported immediately to FM help desk.

Date Reported	Camera No.	Fault Details/ Action Taken	Date Repaired

Appendix H – Incident, view & disclosure log

Record Log of CCTV Viewing / Removal of Recorded Images

Staff should also record any incident viewed as an aid to subsequent investigations and report to management e.g. a car parking collision, visitor slipping on ice etc.

Date & Time of Removal & Viewing	Date & Time of any Image Return	Name of Officer Providing or Removing Images	Person Taking or Viewing Images	Reason for taking or viewing Images (include location, camera number, date time etc.)	Outcome (if any)
		Print: Sign:			
		Print: Sign:			
		Print: Sign:			
		Print: Sign:			