Policy A11 - CCTV

Objectives

To protect the Academy buildings and assets
To increase personal safety and reduce the fear of crime
To support the Police in a bid to deter and detect crime
To assist in identifying, apprehending and disciplining offenders
To protect members of the public and private property

Contents

1. Introduction 2
2. Statement of Intent 2
3. Siting the Cameras 3
4. Covert Monitoring 3
5. Storage and Retention of CCTV images 3
6. Access to CCTV images 4
7. Subject Access Requests (SAR) 4
8. Access to and Disclosure of Images to Third Parties 4
9. Complaints 4
10. Further Information 5
11. Policy Status and Review 5

Appendix A – Declaration Checklist 6

Appendix B – CCTV Signage 7

Appendix C – General Data Protection Regulation 2018 8

Appendix D - Academy CCTV Impact Assessment for the use of surveillance CCTV (including sample answers for information) 9

Appendix E – Viewing Logs of stored CCTV images 13

1. Introduction

1.1 This policy outlines the University of Brighton Academies Trust's approach to the use of CCTV at its academies and Central offices, and how it complies with the General Data Protection Regulation (2018).

1.2 Each Trust site may use closed circuit television (CCTV) images to monitor the buildings and grounds up to their boundary in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to assets, resources and property as long as you have a 'lawful basis' to do so under the General Data Protection Regulation (GDPR) .

1.3 The CCTV system may comprise of any number of internal and external fixed, mobile, PTZ, wired or wireless cameras.

1.4 Systems may have sound recording capability, but if cameras have this capability the recording device must not be able to pick up conversations of neighbouring properties or land and or any other public area outside the academy boundaries. If sound recording systems are installed it must be done so in consultation with staff and the affected communities.

1.5 The CCTV system is owned and operated by the academy or Trust relevant to where it is situated. The deployment of cameras is determined by Senior Leadership Team's.

1.6 The CCTV is used by academy or Trust Senior Leadership Team only and in a limited delegated capacity by the Facilities Management officers. The Senior Leader at each location or their appointed representative has overall responsibility as the designated Data Controlling Officer.

1.7 The further introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and affected communities.

1.8 All authorised operators and employees with access to images must be aware of the procedures that need to be followed when accessing the recorded images. All operators must be aware of their responsibilities under the CCTV code of practice (ico.org.uk) . All employees must be aware of the restrictions in relation to access to, and disclosure of, recorded images.

2. Statement of Intent

2.1 Each academy will seek to comply with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Data Protection Act 1998. This guidance has yet to be amended to reflect GDPR changes (09/19) but is intended to ensure CCTV is used responsibly and provide the Trust as employer with trust and confidence in its continued use. In addition, the ICO provides CCTV system operators with a CCTV Data Protection self-assessment and this can be accessed from the following link; https://ico.org.uk/for-organisations/data-protection-self-assessment/cctv-checklist/ All sites operating CCTV are advised to complete the self-assessment, which will rate your current practice, advise on actions and provide further guidance.

2.2 Each academy will treat the system and all information, documents and recordings obtained and used as data which are protected by the General Data Protection Regulation.

2.3 Cameras may be used to monitor activities within the site boundary and on land owned by the Trust to identify criminal activity occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the staff, pupils and visitors.

2.4 Unless an immediate response to events is required, staff must not direct cameras at private property, an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Powers Act 2000 (legislation.gov.uk)

2.5 CCTV warning signs will be clearly and prominently placed at all external entrances to each premises where CCTV is operational, including the boundary entrances if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see Appendix B). In areas where CCTV is used, there will be prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

2.6 The planning and design of the system should provide maximum effectiveness and efficiency, but it is not possible to guarantee that a system will or can cover or detect every single incident taking place in the areas of coverage.

2.7 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recorded materials will only be released to the media for use in the investigation of a specific crime and with the written authority/request of the Police. Recorded materials will never be released to the media or social media for purposes of entertainment.

3. Siting the Cameras

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. For example, cameras will not be placed in areas which are reasonably expected to be private such as toilets. Each academy will ensure that the location of equipment is carefully considered to ensure that images captured comply with the General Data Protection Regulation.

3.2 Each CCTV installation will position cameras so that their coverage is restricted to Trust owned premises and grounds.

3.3 CCTV will not be used in classrooms or offices, except in exceptional circumstances (see Covert Monitoring below).

3.4 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4. Covert Monitoring

4.1 In exceptional circumstances a site may wish to set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or serious unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances' authorisation must be obtained from the the Executive Director of Strategy

4.3 Covert Monitoring may take place when circumstance 4.1 (i.) and 4.1 (ii.) are satisfied. Covert Monitoring will never be used to observe or assess a member of staff's professional performance, or to contribute to capability proceedings.

4.4 Covert monitoring must cease following completion of an investigation.

4.5 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

5. Storage and Retention of CCTV images

5.1 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[1].

5.2 All retained data will be stored securely.

[1] 'The DPA does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose' (Information Commissioner's Office CCTV Code of Practice*:* surveillance-by-consent-cctv-code-update-2015-jonathan-bamford-20150127.pdf (ico.org.uk) *In the picture - A data protection code of practice for surveillance cameras and personal information*.

6. Access to CCTV images

6.1 Access to recorded images will be restricted to those staff authorised to view them, and outside agencies such as the Police and will not be made more widely available.

6.2 The ability to view live and historical CCTV data available via network software is only to be provided at designated locations and to authorised persons only.

7. Subject Access Requests (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the General Data Protection Regulation.

7.2 All requests should be made in writing to the Senior Leader or their representative. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 SAR requests will be responded to as soon as possible and no longer than within 40 calendar days of receiving the written request and any fee.

7.4 A fee cannot be charged for an SAR, except under very specific circumstances (See the ICO site re: Right of access/subject access requests and other rights | ICO")

7.5 The Academy reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

7.6 SAR requests will be dealt with as per the Right of access | ICO.

8. Access to and Disclosure of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers where these would reasonably need access to the data (e.g. Incident investigators).

8.2 Requests should be made in writing to the Senior Leader responsible for the system or their representative.

8.3 The data may be used within the Trust's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

8.4 When it is within the power to decide whether or not to disclose information to the police, that disclosure of information will be at the discretion of the Academy Principal / Service Head and the Head of Marketing and Communications for the Trust.

9. **Complaints**

9.1 Complaints and enquiries about the operation of CCTV should be directed to the Principal of that Academy or the Service Head in the first instance.

10. Further Information

10.1 For further information on CCTV and its use please see below:

- General Data Protection Regulation 2018
- Regulation of Investigatory Powers Act (RIPA) 2000
- Protection of Freedoms Act (POFA) 2012
- Information Commissioner's Office (ICO) CCTV Code of Practice is published at: CCTV code of practice (ico.org.uk)

11. Policy Status and Review

Written by:	Estates and Facilities Management Director
Owner:	Estates and Facilities Management Director
Status:	V1 Approved
Approval date:	V1 1/7/15 (Board of Directors) Merger editorial changes 1 September 2017
Review Date:	By 2020/21 – Reviewed for GDPR July 2018 Sept 2019 – Reviewed and updated by DS for conformity and to cover central offices. Oct 21 – General review and update for regulatory compliance

Appendix A – Declaration Checklist

This CCTV system located at …… and the images produced by it are controlled by the Principal / Service Lead or their representative who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the General Data Protection Regulation 2018).

The …… Academy/Department have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of users. It will not be used for other purposes. We conduct an annual review of our use of CCTV to ensure its compliance.

ACTIONS	Checked: (Date)	By: (Name)	Date of next Review:
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required			
Staff and affected members of the community will be consulted about the proposal to install further CCTV equipment			
Cameras have been sited so that they provide clear images			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

A copy of this declaration is available as part of academy compliance requirements in the Parago software. and must be completed at least annually or when a significant change or has addition to the CCTV system has occurred.

Sent to: …… **By:** …… **Date:**……

E&FM Office Use Only –

Received by: …… Date:……

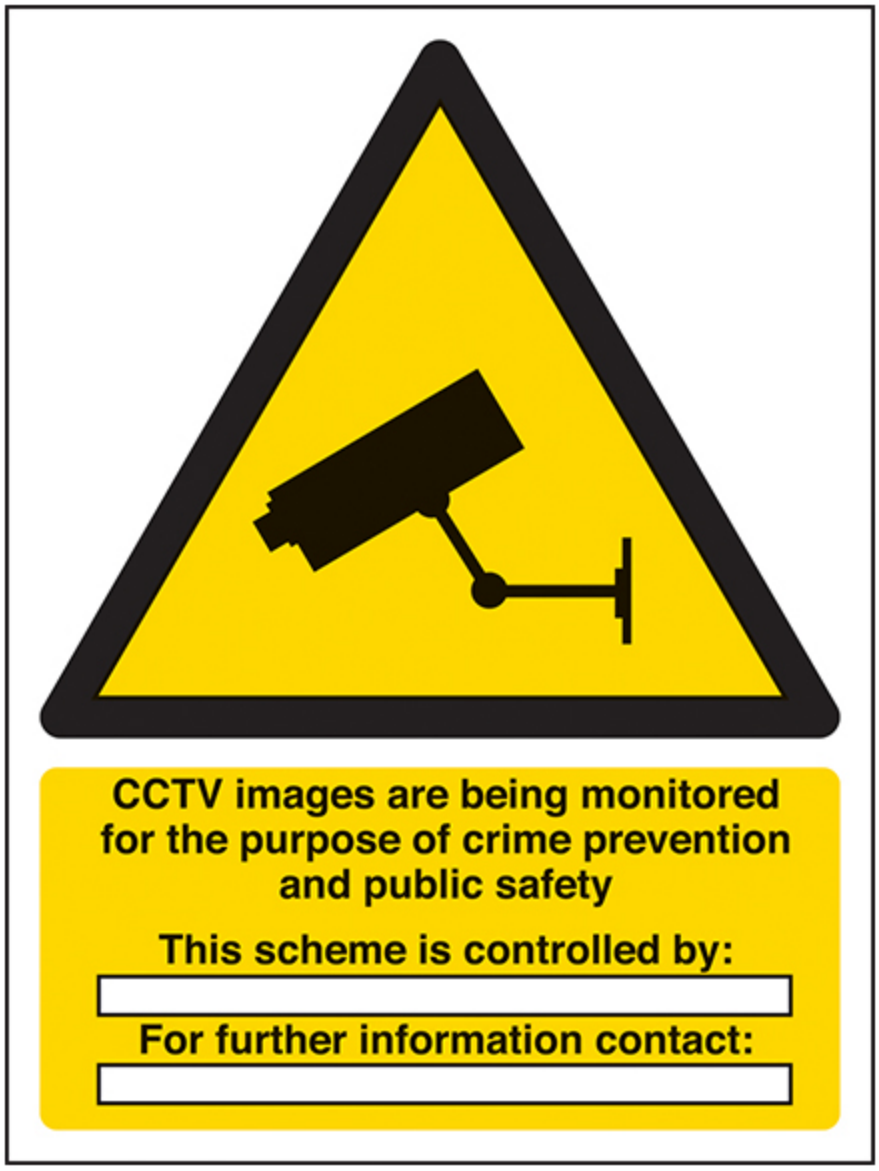
Appendix B – CCTV Signage

It is a requirement of the General Data Protection Regulation to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The Academy is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That CCTV surveillance is in operation in this area and that pictures are recorded
- The purpose of using CCTV
- The details of the organisation operating the system if not obvious

Example of suitable signage -



Appendix C – General Data Protection Regulation 2018

The General Data Protection Regulation 2018: Key Principles

Article 5 of the GDPR requires that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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; and

f) 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.”

Article 5(2) requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

This is not a full explanation of the principles, for further information refer to the ICO outline of the General Data Protection Regulation.

University of Brighton

Academies Trust

Appendix D –

CCTV Impact Assessment for the use of surveillance CCTV (including sample answers for information.

Location	(Academy/office name here)
Assessment carried out by:	(Name and job title)
Assessment effective from:	(Date effective from)
Assessment effective to:	(Date effective to)
Our Data Controlling Officer:	(Name and job title, contact details) Principal or Service Lead
Registration with the Office of the Information Commissioner Last updated on and by whom:	(Date and Name and job title)
Date when checks for serviceability of CCTV systems and clarity of images last completed and by whom:	(Date and Name and job title)

Camera information

Areas covered by installed surveillance CCTV, whether active or not. (This should include all outside areas and grounds, all entrances, all internal areas, individually stated where possible. Total number of possible operative cameras should be included. The use of a site plan to identify areas and locations may be more effective and relevant to users.

CAMERA AREA	No.		CAMERA AREA	No.

Generic Impact Assessment for the use of CCTV in area……

Purpose(s) for use of surveillance CCTV:

The purpose of using CCTV is to protect staff, students, visitors and property from the actions of individuals. These actions may not necessarily be criminal offences but will have a negative impact on teaching, learning and employees' working environment. As a site with around ……. students and a multi-level building, monitoring behaviour using staff alone can be a challenge. CCTV images are recorded so that they can be used to establish who committed an offence. The CCTV recordings are used alongside traditional ways of investigating such as obtaining witness statements.

Advantages of use of CCTV over other possible methods:

Enables staff to concentrate on teaching and learning. It is not reliant on staffing availability and it is operational at times of the day that the building is unoccupied.

Assessment of amount of equipment used and time equipment is active:

The equipment has been chosen to provide the maximum coverage in the area it is situated, reducing the number of overall cameras. The equipment has been evaluated for its ability to provide the required image clarity to identify individuals. The equipment is active for 24hours a day, seven days a week.

Specific ways in which data collected will be used, including restrictions:

Images will be used to investigate reports of crime, including vandalism, intimidation and theft and to monitor student behaviour. It is also a tool for investigating accidents and incidents on the Academy buildings and grounds.

Data will not be used to monitor individuals working practices, check timekeeping or to covertly monitor without the permission of the Principal and will only be relevant to the investigation that has been requested.

For stored data, the method used, the maximum length of time of storage, and how the data might be used:

All data will be stored digitally. The data will be stored for up to 30 days to allow an incident to come to light and be investigated. The data maybe used by outside services and authorities such as the police in relation to the investigation of crime against property or an individual.

All personnel having <u>immediate</u> access to data collected and stored, as part of specific duties:

The Senior Leadership Team – List names
The Site Manager – (live images only)
Etc. etc.

The CCTV Servicing Company
– Bloggs CCTV

Nominated Data Processor ……

Details of how data may be processed, by whom and what purpose(s):

Data may only be processed by the nominated person above. Data can be stored to disk or another digital format for the purposes of a police request for information or to take the stored data to a third party for identification purposes, after which the data will be erased.

Details of further personnel who may gain temporary access to data as part of their duties:

Administration and Teaching Staff who would require written authorisation from the Senior Team to access the system and be issued with a temporary access code

Methods of notification of the presence of surveillance CCTV and other information channels:
There is visible signage at each camera location and the Academy community has received a copy of the Academies CCTV policy outlining use and access.

Details of all method(s) by which images, or collected data, from CCTV may be streamed to any outside agency or other parties, if relevant. Restrictions on access are also included:
Data may be streamed to remote handheld devices in exceptional circumstance to authorised personnel such as the police.

Where an outside agency is entirely responsible for the operation and control of the CCTV equipment, it's monitoring and the collection and use of data collected, all relevant and necessary details: N/A

Assessment of any possible impact of CCTV surveillance on the right to privacy, performance or general well-being of any individuals:
CCTV has been located in areas that do not impact on privacy of student's staff and visitors. CCTV in toilet areas is limited to the hand wash area and does not look into cubicles or changing areas. CCTV will not be used to monitor staff performance.

Other relevant information:
Although we have not surveyed people, we believe the following to be correct: Staff are aware that they are under surveillance and know that it is for their protection and not to monitor them working. Students feel protected having CCTV and we know that some park their bikes in front of cameras to keep them safe.

A separate sheet should be completed for each area, giving precise details of the use of surveillance CCTV and the data collected from that area. It may be adequate to group together some areas where the information to be recorded is entirely or partially common, without loss of specific reference.

Appendix E- Viewing Log of stored CCTV images –

Date Stored	Who by	Log Number / Crime Ref Number	Please state the format these images are being stored (e.g. CD ROM/Hard Drive/Flash drive)	Please state the date the footage was destroyed, by whom and why.	Signed off by Manager Name, Position and Date.

3rd Party viewing log

Date & Time of viewing	Name/s of the person/s viewing the images & the organisation they represent	State the reasons for the viewing	Images viewed (state location, date and time of original image/s)	The outcome if any of the viewing	Date and time the images were returned for storage/destroyed