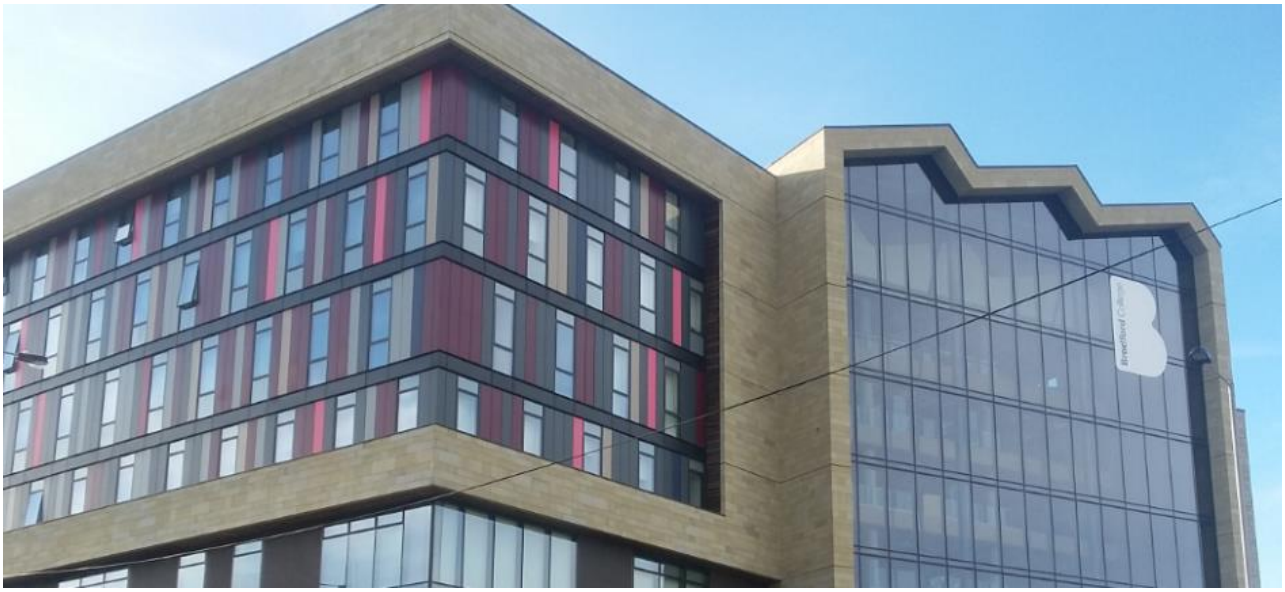

Closed Circuit Television (CCTV) Surveillance and Monitoring Policy 2019

Bradford College

Document change control

Document title:	Closed Circuit Television (CCTV) Policy 2019
Audience:	14-16 year old students; FE students; HE students; Permanent Academic Staff (incl. part time hourly paid); Apprentices; Professional Support Staff, Temporary/Contracted Staff, CTS and Forster College Staff/Assessors and Stakeholders
Version:	2
Approved by:	Executive Leadership Team
Date approved:	May 2019
Date of next review:	May 2020
Document author(s):	Estates & Facilities Manager
Date issued:	May 2019
Document reference:	EAP03

Revision history

Version	Type (e.g. replacement, revision etc…)	Date	History (reason for changes)
1	New	June 2015	
2	Revision	May 2019	Update in line with GDPR

Monitoring and review

- This policy will be reviewed by the Executive Leadership Team at least annually.

1. Introduction

a) The Bradford College Group "the College" has in place a CCTV surveillance system "the CCTV system" across its campuses. This policy details the purpose, use and management of the CCTV system at the College and details the procedures to be followed in order to ensure that the College complies with relevant legislation and the current Information Commissioner's Office Code of Practice.

b) The College will have due regard to the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the College will also have due regard to the Home Office Surveillance Camera Code of Practice 2014, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/368115/Leaflet_v6_WEB.pdf

c) This policy is based upon guidance issued by the Information Commissioner's Office, 'In the picture': A data protection code of practice for surveillance cameras and personal information'1 ("the Information Commissioner's Guidance").

d) This policy and the procedures therein detailed, applies to all of the College's CCTV systems including body worn cameras, webcams, covert installations and any other system capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals. CCTV images are monitored and recorded in strict accordance with this policy which details how we will deal with requests for covert surveillance by Law Enforcement Agencies.

2. Owner

a) The CCTV System is owned by the Bradford College Group. The Head of Facilities Management will be the senior point of contact, and is responsible for the day-to-day operation of the CCTV System and ensuring compliance with this CCTV Policy.

b) Contact details:

Head of Facilities Management
Bradford College
Great Horton Road
Bradford
West Yorkshire
BD7 1AY
Telephone: 01274 43 3075

3. CCTV System overview

a) The CCTV System includes 405 cameras over 10 buildings (this may alter due to operational changes as governed under the ICO Guidance and/or POFA Code of Practice and any changes to that guidance).

b) The CCTV System runs 24 hours a day, 7 days a week and comprises fixed position cameras, pan tilt and zoom (PTZ) cameras, monitors, multiplexers (i.e. a device which

allows video signals from multiple CCTV security cameras to be combined and display the multiple video streams on one monitor), digital recorders and signs notifying individuals to the use and operation of the CCTV System. From time to time covert cameras may be used (where such use is permitted by law) for the protection of students, staff, visitors or campus buildings.

c) Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and other members of the public that the CCTV System is in use. They will also provide contact details for the security control room and will explain the purpose of the CCTV System. It is a requirement to notify people entering a CCTV protected area that the area is monitored by CCTV and that images are recorded.

d) Although every effort has been made to ensure maximum effectiveness of the CCTV System it is impossible to ensure that every incident will be seen or recorded.

4. Purposes of the CCTV System

The principal purposes of the College's CCTV system are the prevention, detection and investigation of crime (Law Enforcement Agencies) and Health and Safety purposes (Health and Safety Executive, Enforcement Agencies, Emergency Services).

a) The CCTV system will be used to observe the College campuses and areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

b) The College seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy:

i. for the prevention, reduction, detection and investigation of crime and other incidents;

ii. to ensure the safety of staff, students and visitors;

iii. to assist in the investigation of suspected breaches of College regulations by staff or students;

iv. the monitoring and enforcement of traffic related matters.

5. Control room

5.1 Authorised access

a) Other than Security Control Room personnel, access to the Security Control Room will be limited to authorised Security personnel only, the Head of Facilities Management and authorised members of senior management, police officers *(only if the police have legal grounds to view CCTV footage)* and any other person with statutory powers of entry, as permitted by this CCTV Policy.

b) Images captured by the CCTV System will be monitored and recorded in the Security Control Room, twenty-four hours a day throughout the whole year.

c) Images captured will be dependent upon the positioning of any PTZ cameras at the time of the incident as well as any repairs, maintenance and servicing works are being undertaken.

d) Monitors are not visible from outside the control room.

5.2 Unauthorised access

a) No unauthorised access to the Control Room will be permitted at any time

b) No member of college or security staff shall permit, or seek to permit, any unauthorised person to access the Control Room.

5.3 Staff access

a) Staff may be granted access to the Control Room on a case-by-case basis and only then on written authorisation from the Head of Facilities Management and/or Data Protection Officer.

b) Where necessary for any purpose detailed in this CCTV Policy, 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 enter the Control Room. For example, where there is imminent risk to the safety of anyone within the college or the college buildings themselves. Or if a judgement is made there is an immediate necessity for the prevention, detection and investigation of crime whereby usual disclosure requests could cause serious impact or unnecessary delay to a live crime scene.

c) Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to sign in on the signing in book, which shall include details of their name, their department or organisation they represent and the times of entry to and exit from the centre. The control room will also log any access to the control room.

d) Under no circumstances must staff access or attempt to obtain CCTV images for their own personal use or gain for example to establish the identity of other car park users or to ascertain arrival or leaving times of team members or colleagues. All requests must be in line with college policies and procedures.

6. Monitoring and Recording

a) Cameras are monitored in the Security Control Room, which is a secure area. The Control Room is equipped with a licensed radio system linking it with uniformed Security Officers who provide foot and mobile patrols and are able to respond to incidents identified on CCTV monitors.

b) The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked daily to ensure that the images remain fit for purpose.

c) All images recorded by the CCTV System remain the property and copyright of the College.

d) The monitoring of staff activities can only be requested via a member of the HR Team who will contact the appropriate person to obtain any CCTV footage.

e) The use of covert cameras will be restricted to rare occasions, when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of the Data Protection Officer (in consultation of the Head of Facilities

Management) will be sought before the installation of any covert cameras. The Data Protection Officer and the Head of Facilities Management should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert recording.

f) Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there is reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period. *(see section 7 relating to covert recording)*

g) Body worn cameras may be used during Security patrol duties. The downloading of images from such cameras will only be conducted by trained security staff and cameras will be cleansed following each shift.

h) Security staff wearing body worn cameras will disclose, when approaching any individuals or groups of individuals, they are being recorded with both imagery and audio.

7. Covert Recording

a) Where permitted to do so under relevant laws and regulations, covert cameras may be used by Bradford College under the following circumstances and on the written authorisation of the DPO. Where necessary, such as in the case of Law Enforcement requests, or where our policies and procedures do not allow, the Data Protection Officer may seek legal advice to establish the legality of a request for covert monitoring and surveillance.

   i. Where there is a reasonable cause to suspect activity is taking place or is about to take place that may seriously or substantially affect the operation of Bradford College;

   ii. If informing the individuals concerned that recording was taking place (or is to about to take place) would seriously prejudice the objective of making the recording.

b) Prior to the Data Protection Officer granting authorisation to use covert surveillance, the requesting applicant (e.g. law enforcement agencies, regulatory bodies or Bradford College management) must have demonstrated and documented that all reasonable procedures and practices were put in place to prevent suspected illegal or unauthorised activity from taking place and that there are legal grounds to use covert surveillance and monitoring.

c) External requests from law enforcement agencies and other regulatory bodies (Police, National Crime Agency, Counter Terrorism Unit etc.) must be put in writing to the Data Protection Officer citing the purpose and legal grounds for the request. We will not actively seek to be obstructive to the detection, prevention and investigation of crime, we do have to work within the data protection regulatory framework and consider the rights of the individuals and therefore we will insist on an official request based on current regulatory requirements such as those set out in the CCTV Code of Practice. Any such requests will be reviewed by our legal advisers.

d) Any such covert surveillance will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

e) The decision to adopt covert surveillance will be fully documented and will set out how the decision to use covert surveillance was reached and by whom.

8. Compliance with Data Protection Act 2018 & General Data Protection Regulation (GDPR)

From 25th May 2018, the College will comply with the Data Protection Act 2018 & GDPR. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be:

i. Processed lawfully, fairly and in a transparent manner

ii. Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

iv. Accurate, and where necessary, kept up to date

v. Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed in a manner that ensures appropriate security of the personal data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9. Monitoring Compliance

a) All personnel in the operation of the College's CCTV Systems will be made aware of this policy and will only be authorised to use the CCTV System in a way which is consistent with the purposes and procedures contained therein.

b) All personnel with the responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake GDPR training.

10. Applications for Disclosure of Images

a) Applications by individual data subjects

i. Requests by individuals for images relating to themselves "Subject Access Request" (SAR) should be submitted in writing to the College's Data Protection Officer together with proof of identification.

ii. In order to locate the images, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

iii. Where the College is unable to comply with a SAR without disclosing personal data of another individual who is identified or identifiable from that information, the College is not obliged to provide such information.

b) Access to and disclosure of images to third parties

i. Non routine requests for images should made in line with our Data Protection (GDPR) Policies and Procedures via the Data Protection Officer.

ii. Routine requests (those determined by college policies and procedures and our Privacy Notices such as internal requests by authorised staff) should be made to the Head of Facilities Management who will liaise with Data Protection Officer as to the validity of the request where necessary.

iii. In limited circumstances it may be appropriate to disclose images of a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in circumstances where an exemption applies under relevant legislation.

iv. Such disclosures will be made at the discretion of the Data Protection Officer with reference to the relevant legislation and where necessary, following advice from the Data Protection Officer.

v. Where a suspicion of misconduct arises and at the formal request of an HR Advisor, the Head of Facilities Management.

vi. The Head of Facilities Management may provide access to CCTV images to Investigating officers when sought as evidence in relation to student discipline cases.

vii. A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for disclosure.

viii. At the end of each month copies of all DSAR's are to be sent to the Data Protection Officer in an encrypted format.

11. Recording and Retention

a) In accordance with the ICO Guidance and data protection legislation, information recorded by the CCTV System will be stored in a way that maintains the integrity of that information, to ensure that the rights of individuals recorded by the CCTV System are protected and that the information can be used effectively for its intended purpose.

b) Images will be recorded and normally held for no more than 30 days, after which time they will be erased.

c) Longer retention periods may be used where lawful to do so and such longer retention is necessary for the purpose(s) for which the information was recorded, in accordance with this CCTV Policy. Further, any such longer retention periods will need to be authorised by the College Data Protection Officer and, in specific cases or investigations, logged accordingly and the eventual date of erasure also recorded.

12. Concerns about your personal information and use of CCTV

a) Concerns in relation to the processing of personal data and the use of CCTV Surveillance and Monitoring, or the way your data privacy rights have been handled, can be directed to the Data Protection Officer in the first instance to enable us to investigate the

concern(s). We will aim to carry out the internal review as soon as possible in line with ICO requirements.

b) If you are dissatisfied with our response or if we fail to review your concerns, you have the right to escalate your concern directly to the Information Commissioner's Office (ICO). The ICO provides an online facility for reporting complaints which you will find at https://ico.org.uk/concerns/.

13. Contact

If you have any feedback about this policy please contact the Data Protection Officer:

By Post

Data Protection Officer
Bradford College
Great Horton Road
Bradford BD7 1AY

Email: dataprotection@bradfordcollege.co.uk
Telephone: 01274 433333