CCTV Policy
2020-22

Responsible Officer:	Vice Principal Corporate Services
Date:	December 2020
Review date:	December 2022 (unless preceded by legislation)
Procedure available:	Intranet/Website
Approved by:	Executive

1. Purpose and Scope

It is the policy of the College to provide a safe work environment for employees, students, visitors, temporary staff and contractors while on the College premises and within the College buildings.

CCTV cameras are deployed at various locations within and around the College estates, to assist in the prevention and detection of crime, and to increase the safety of staff, students and visitors on College premises.

This policy details the operating standards and procedures for closed circuit television (CCTV) systems installed at the Buckinghamshire College Group, in accordance with the requirements of:

- General Data Protection Regulation (GDPR)
- The CCTV Code of Practice 15/10/2014 issued by the Information Commissioners Office.
- Article 8 of the Human Rights Act Right 1998. Respect for Private and Family Life.

2. Operating Principles.

To ensure compliance with the above, all CCTV operations, must at all times, adhere to the following principles.

- Fairly and lawfully processed.
- Adequate, relevant and not excessive.
- Accurate.
- Images are not retained for longer than is justifiably necessary.
- Processed in accordance with the individual's rights.
- Secure.

3. Rights in relation to Automated Decision Taking

Article 22 of the GDPR.

Buckinghamshire College Group CCTV system is not used in any manner in relation to automated decision taking.

4. Operational Management

The CCTV operation management is the responsibility of the Head of Estates or the Deputies.

5. Data/Privacy Protection

The College named Data Protection Officer is Executive Director of MIS and Planning.

The Head of Estates is the authority with regard to requests under the terms of the Freedom of Information Act and requests from Data Subjects (persons whose images have been recorded by the system).

Data Controller:
Executive Director MIS & Planning

6. CCTV Control of Viewing and Access to Data.

All viewing and observing of the CCTV images will be carried out at Buckinghamshire College Group on the appropriate campus. No unauthorised access to the CCTV screens will be permitted at any time. Access will be strictly limited to the duty security officers the Data Protection Officers or the Data Controllers. Images saving to other formats such as DVD discs will only be carried out using the computer on the Head of Estates desk or in the IT office.

CCTV viewing or observing in other places will only take place if authorised by a Data Controller. This includes remote viewing.

All staff working in the viewing area will be made aware of the sensitivity of handling CCTV images and recordings. The Head of Estates will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

Contractors working on the system will sign an undertaking that they understand and will comply with Buckinghamshire College Group, CCTV Policy through the contractor management procedure.

Images are retained on a secure hard drive for up to 30 days but more likely to be 14 days; after this period, they are automatically over written.

Subject to the appropriate data subject access requests, images are normally copied to a discs, which is then given to the requesting organisation or individual. The downloads are recorded in the CCTV folder which is located in the Estates Office and is signed by the receiving authority/person. In order to carry out this process, images are initially copied to a secure drive within the college system. Should there be any further requests, or if there has been a technical issue, these images are retained on the Head of Estates drive for up to 12 months for reasons of ensuring footage is available for any resulting court action.

7. Access to/Disclosure of CCTV images

Access or disclosure requests will only be authorised by a Data Protection Officer or a Data Controller and must be received within 14 days of the footage being taken.
Requests for access to, or disclosure of (i.e. provision of a copy), images recorded on the College CCTV systems from third parties, will only be granted if the requestor falls within the following categories.

1. Data subjects (persons whose images have been confirmed as recorded by the CCTV systems).
2. Footage of other personal data (images of others) are not disclosed.
3. Law enforcement agencies.
4. An authorised College member who has responsibility for student discipline - in the course of a student disciplinary investigation.
5. An authorised member of College staff in the investigation of a Health and Safety at Work Act incident.
6. An authorised member of staff in the investigation of crime.
7. An authorised member of staff in the investigation of process
8. Relevant legal representatives of data subjects.

8. Access to images by a law enforcement agency

Law enforcement agencies may view or request copies of CCTV images subject to providing an appropriate written General Data Protection Regulation request and in accordance with the protocols contained within this document. In very urgent serious cases of crime or public safety, relevant law enforcement agencies may view CCTV images if requested in person and subject to authorisation by one of the Data Controllers. Requests will need to be made within 14 days of the footage being taken, after this date, it is unlikely it will be available.

9. Access to images by a subject

CCTV digital images, if they show a recognisable person, or any other identifying details (e.g. Registration plates), are personal data and are covered by the General Data Protection Regulation. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

Additionally, persons may make a Freedom of Information Act request.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to and received by the Data Protection Officer within 14 days of the footage being taken. All applications must be made by the Data subject themselves, or their legal representative.
Requests will be processed promptly. Freedom of Information request will be responded to within 20 working days.

The General Data Protection Regulation gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, or the images have been erased. If a data subject access request is refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

The Freedom of Information Act 2000 gives the Data Protection Officer exemptions under Section 40 and 38 of that act which would prevent disclosure of CCTV images. If a refusal is made under these exemptions, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

10. Right to prevent processing likely to cause damage or distress

The Right to Object within the General Data Protection Regulation

An individual has the right to request to cease, or not to begin processing, or processing for a specified time period or in a specified manner, where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

Such requests must be made in writing to the Data Protection Officer, who will provide a written response within 21 days of receiving the request, stating his reasons as to regarding the data subject notice as to any extent unjustified and the extent (if any) to which he has complied or intends to comply with it.

11. System Details

Any changes or additions to the system will be in compliance with the General Data Protection Regulation and the Information Commissioners Office CCTV code of practice.

Buckinghamshire College Group CCTV has a number of cameras on the grounds at each campus with images being transmitted to a secure server for storage and for recall at a later date, with a live feed being streamed from the server to the Security Officers monitor and the Estates Office in each of the College Buildings.

The College system consists of: Fixed position cameras, pan and tilt cameras, 360^{o} cameras.

Cameras are located at strategic points in each campus and across the grounds. They cover vulnerable points such as entrance and exits to buildings. No cameras cover any areas which would be considered private.

The system is capable of recording audio on some of the positions.

A detailed plan locating each camera will be documented and available in the Estates Office.

There are signs prominently placed at each main entrance/exit points to each building informing that a CCTV installation is in use.

Equality Impact Statement
We have a duty to consider the impact of changes on groups with Protected Characteristics (race, disability, age, sexual orientation, religion or belief, gender reassignment, pregnancy and maternity, marriage and civil partnership).

What are the overall aims of the change? Why are you proposing it?	The aim of this policy is to provide guidance and procedures to ensure that all are in place with a view to protect the users of the College
Given the aims of your proposal, what issues does your data/information highlight?	Everybody is included within this policy, and all groups are given equability in regards to their needs and provisions
How could the proposed change affect positively/negatively on groups with protected characteristics?	No one is impacted in a negative way. This has a positive impact on all groups, as they are ensured equal treatment in their security
What actions will you take to mitigate any negative impact?	No negative impact to having this policy
Is there any potential negative impact justified in light of wider benefits of the proposal	No negative impact to having this policy
Recording final decision	This policy requires Executive approval
Has the policy taken into consideration the requirements of GDPR regulations? Are there any actions that need addressing, e.g.; data sharing agreement; has data consent been considered; data retention timescales?	GDPR regulations have been considered and actions comply with data protection requirements.