



CCTV Policy

Policy no:	HSE 4.4
Version no. & date:	Version 1.1 – 23 October 2026
Author:	Estates Manager
Last review date:	23 October 2026
Next review due:	October 2028
Responsible Committee:	College Management Team (CMT)
Approved by & date:	College Management Team (CMT) – 23 October 2026
External reference points:	UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018 Human Rights Act 1998 Surveillance Camera Code of Practice (Home Office) ICO CCTV and Video Surveillance Guidance ICO Guide to Data Protection
Linked policies:	DIG 2.1 Data Protection and Confidentiality Policy; DIG 2.3 Student Privacy Notice; DIG 2.4 Records Management and Data Retention Policy; DIG 2.6 Information Security and Acceptable Use Policy; DIG 2.7 Subject Access Request and Individual Data Rights Policy
Audience:	All staff, students, contractors and visitors

1. Purpose

UK College of Business and Computing (UKCBC or the College) operates Closed-Circuit Television (CCTV) systems to support the safety and security of staff, students, visitors and property across its premises. This policy sets out the framework governing the installation, operation, management and review of CCTV systems at the College.

CCTV is used to prevent and detect crime, monitor access to buildings and facilities, and protect assets where there is a clear and justified need. The College only deploys CCTV where it is necessary, proportionate and for a defined purpose. The use of surveillance must balance security requirements with the rights and freedoms of individuals, in accordance with data protection law.

2. Scope

This policy applies to all CCTV systems operated by UKCBC across its UK premises. It covers the capture, storage, use and disclosure of recorded images and applies to:

- all staff, students, contractors and visitors who may be recorded by CCTV systems;
- all personnel authorised to operate or access CCTV footage; and
- any third-party service providers engaged in the operation or maintenance of CCTV equipment.

This policy does not extend to covert surveillance or body-worn cameras, which would be subject to separate consideration and approval if the College were to introduce such measures.

3. Definitions

CCTV (Closed-Circuit Television): A video surveillance system used to capture and record images of individuals and areas for security and safety purposes.

Personal data: Any information relating to an identified or identifiable individual, as defined under UK GDPR.

Data controller: The organisation that determines the purposes and means of processing personal data. UKCBC acts as the data controller for all CCTV footage captured on its premises.

Data Protection Officer (DPO): The individual designated to oversee data protection compliance. At UKCBC, DPO functions are currently held by the Academic Registrar.

Authorised personnel: Staff formally designated by the Estates Manager and Head of IT to operate or access CCTV systems.

Proportionality: The principle that surveillance must not be excessive relative to the legitimate aim it serves.

Data Protection Impact Assessment (DPIA): A process to identify and minimise data protection risks, required where processing is likely to result in a high risk to individuals.

4. Legal Framework

CCTV systems capture images of individuals and therefore constitute the processing of personal data. The College operates all CCTV systems in compliance with:

- UK General Data Protection Regulation (UK GDPR), which requires that personal data is processed lawfully, fairly and transparently, and only for specified, explicit and legitimate purposes;

- Data Protection Act 2018, which supplements UK GDPR and provides the domestic legislative framework;
- Human Rights Act 1998, which protects the right to respect for private and family life under Article 8 of the European Convention on Human Rights; and
- Surveillance Camera Code of Practice (Home Office), which provides guidance for operators of surveillance camera systems in public spaces.

The College also has regard to ICO guidance on CCTV and video surveillance when designing, deploying and reviewing its systems.

5. Roles and Responsibilities

5.1 Operations Committee

The Operations Committee has formal oversight of this policy and is responsible for approving it and any subsequent revisions. The Committee receives assurance that CCTV systems are operated in compliance with legal and regulatory requirements.

5.2 Chief Academic Officer (Policy Owner)

The Chief Academic Officer is responsible for maintaining this policy, ensuring it is reviewed in accordance with the review cycle set out in Section 13, and coordinating any required updates in response to legislative or operational change.

5.3 Estates Manager

The Estates Manager is responsible for the day-to-day operation of CCTV systems, including:

- oversight of camera installation, positioning and maintenance;
- ensuring that adequate signage is displayed at all monitored locations;
- managing authorised access to CCTV footage;
- processing and recording requests for disclosure of footage in accordance with Section 9; and
- ensuring that footage is retained and disposed of in accordance with Section 8.

5.4 Head of IT

The Head of IT is responsible for the technical operation and security of CCTV infrastructure, including:

- maintaining appropriate technical controls to protect stored footage from unauthorised access, loss or misuse;
- ensuring secure deletion of footage at the end of the retention period; and
- supporting Data Protection Impact Assessments where required.

Note: The Management Information Systems (MIS) Manager performs DPO-adjacent functions at UKCBC. The College is aware that this role requires careful management to preserve appropriate independence, consistent with UK GDPR Article 38(6). Any matters requiring independent DPO oversight are escalated to the Chief Academic Officer.

5.5 All Staff

All staff who have access to CCTV footage must:

- handle footage only for the purposes set out in this policy;
- maintain strict confidentiality regarding the content of recorded images;

- report any suspected misuse, data breach or security concern to the Estates Manager and MIS Manager immediately; and
- not copy, distribute or retain footage outside of authorised processes.

6. Principles of Use

The College operates all CCTV systems in accordance with the following principles, which are aligned to the data protection principles set out in UK GDPR Article 5.

Purpose limitation: CCTV is used only for the purposes for which each system is established. The purpose of each camera must be clearly defined and documented before installation.

Proportionality: Surveillance must be proportionate to the risks being addressed. CCTV must not be deployed in an excessive manner or in locations where the risks do not justify its use.

Transparency: The College informs individuals that surveillance is in operation through clear signage at all relevant locations. Further information about how CCTV data is used is available through the College's Student Privacy Notice.

Data minimisation: CCTV systems are configured to capture only the data necessary for the stated purpose. Coverage must not extend beyond what is required.

Security: All footage is held securely and is accessible only to authorised personnel.

Accountability: The College maintains records of CCTV deployment, access and disclosures to demonstrate compliance.

7. Justification and Deployment

Before installing or expanding CCTV coverage, UKCBC must assess whether the intended purpose can be achieved through less intrusive means. CCTV is only implemented where alternative measures are insufficient and where there is a demonstrable operational or safety need.

A Data Protection Impact Assessment (DPIA) must be completed before any new CCTV system or significant expansion of existing coverage is deployed. The DPIA must assess the risks to individuals' rights and freedoms and confirm that deployment is justified, necessary and proportionate.

The College must document for each camera:

- the location and area covered;
- the stated purpose and justification for deployment; and
- the expected outcomes and any risks identified.

This documentation is maintained by the Estates Manager and is reviewed as part of the annual compliance review described in Section 13.

8. Location of Cameras

CCTV cameras are installed in areas where there is a clear safety or security justification. These typically include:

- building entrances and exits;
- reception areas;
- corridors and communal areas; and
- locations with an identified and documented security risk.

CCTV must not be used in areas where individuals would reasonably expect a high degree of privacy. Cameras must not be installed in toilet facilities, prayer rooms, changing areas or other locations of a similar nature.

The use of CCTV within staff workspaces requires a documented justification and must be approved by the Chief Academic Officer before installation. Any such deployment must be communicated clearly to staff in advance.

9. Transparency and Signage

UKCBC must ensure that individuals are informed about CCTV operation through clear, visible and legible signage at all monitored locations. Signage must be positioned at entry points and at locations where cameras are deployed.

Signage must include:

- a statement that CCTV recording is in operation;
- the name of the data controller (UKCBC); and
- contact details for further information (dpo@ukcbc.ac.uk).

Further information about how CCTV footage is used, retained and disclosed is provided in the UKCBC Student Privacy Notice and, for staff, in the DIG 2.1 Data Protection and Confidentiality Policy. The Estates Manager is responsible for ensuring signage remains current, visible and compliant.

10. Data Management and Retention

CCTV footage is used only for the purposes for which the system was established. Footage must not be used for any other purpose without explicit authorisation from the Chief Academic Officer.

CCTV footage is retained for a maximum of 30 days, unless it is required for an ongoing investigation, legal proceedings or has been specifically requested by law enforcement. Where footage is retained beyond 30 days, this must be recorded by the Estates Manager, with the reason and anticipated retention period documented.

Footage that is no longer required must be securely and permanently deleted by the Head of IT. Deletion must be recorded in the access and disposal log.

Retention periods for CCTV footage are set out in the DIG 2.4 Records Management and Data Retention Policy. Where there is a conflict between this policy and the retention schedule, the Chief Academic Officer must be consulted.

11. Access and Disclosure

11.1 Authorised Access

Access to CCTV footage is restricted to authorised personnel only. The Estates Manager must maintain an up-to-date access log recording who has accessed footage, when and for what purpose.

11.2 Subject Access Requests

Individuals have the right to request access to CCTV footage in which they appear. The College handles such requests in accordance with the DIG 2.7 Subject Access Request and Individual Data Rights Policy. Where footage also captures images of other individuals, appropriate redaction must be applied before disclosure.

11.3 Disclosure to Third Parties

Footage may only be disclosed to third parties, including law enforcement agencies, where:

- there is a clear lawful basis for disclosure under UK GDPR;
- the request is made in writing and specifies the purpose; and
- the disclosure is approved by the Chief Academic Officer or, in their absence, the Estates Manager.

All disclosures must be recorded in the access and disclosure log, including the identity of the recipient, the purpose and the date of disclosure.

12. Complaints

Any individual who has concerns about the College's use of CCTV may raise them as follows:

In the first instance, concerns should be directed to:

Email: dpo@ukcbc.ac.uk

Post: Data Protection Officer, UKCBC, Eastgate House, 40 Dukes Place, London, EC3A 7LP

The College will acknowledge complaints within five working days and will investigate them in accordance with the College's complaints procedures.

If an individual is not satisfied with the College's response, they have the right to complain to the Information Commissioner's Office (ICO):

Website: www.ico.org.uk | Phone: 0303 123 1113 | Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

13. Monitoring and Review

The Estates Manager is responsible for the operational monitoring of CCTV compliance, including maintaining access logs, signage, and disclosure records.

This policy must be reviewed every two years or earlier if required by legislative change, regulatory guidance, a significant operational change, or a security incident involving CCTV data. The review is the responsibility of the Chief Academic Officer.

An annual compliance review must confirm that:

- each camera installation remains justified and proportionate;
- DPIA documentation is current;
- signage is adequate and legible;
- access logs are being maintained; and
- retention and disposal procedures are being followed.

Outcomes of the compliance review are reported to the Operations Committee.

14. Linked Policies and External References

This policy should be read alongside the following College documents:

- DIG 2.1 Data Protection and Confidentiality Policy v6
- DIG 2.3 Student Privacy Notice v4
- DIG 2.4 Records Management and Data Retention Policy v3
- DIG 2.7 Subject Access Request and Individual Data Rights Policy v4
- DIG 2.6 Information Security and Acceptable Use Policy v3.3a

External reference points:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- Surveillance Camera Code of Practice (Home Office)
- ICO Guidance on CCTV and Video Surveillance

Version History

Version	Date	Author	Summary of changes	Approved by
1.0	May 2026	Pauline Williams	Initial policy; new document prepared for Operations Committee approval.	
1.1	23 October 2026	Chief Academic Officer	Role titles updated following organisational restructure; front sheet, footer and cross references updated for approval; approved by College Management Team (CMT) on 23 October 2026 Title aligned and MIS spelt out in line with GA 3.1 (26 October 2026). Version History table aligned with the suite (26 October 2026).	College Management Team (CMT)