UCG CCTV Policy

This policy outlines how the United Colleges Group uses CCTV (for City of Westminster College and the College of North West London).

Document Status	
Owner	Amanda Thorneycroft
Author	Gavin Prime & Gora Selliah
Date of Origin	03/2022
Colleges Covered	City of Westminster College, College of North West London
Version	2.1
Date of Approval	6th July 2022
Date of Next Review	July 2023
Approval Body	UCG Corporation

GROUP MISSION AND VALUES

The United Colleges Group's vision is to be London's Leading Skills College.

Our Mission is to support economic opportunity through the provision of high-quality education, business solutions and skills for work.

The CCTV Policy supports and underpins the College's values. Our values provide common ground for co-operation to achieve shared aspirations.

- Working together for our learners.
- High quality education and training.
- Improving lives.
- Respect and dignity.
- Honesty and integrity.
- Sustainability.

Further insight into the College's Strategic Plan, which includes detailed explanations on our mission and values, can be found at www.ucg.ac.uk

DEFINITIONS

'the College' refers to United Colleges Group (UCG)

'CCTV' refers to Closed Circuit Television

'DoC' refers to Directors of Curriculum

'ICO' refers to the Information Commissioners Office

POLICY STATEMENT

The College has in place a closed-circuit television ("CCTV") system in campuses to provide a safe and secure environment for students, staff and visitors, and to protect UCG property.

This document sets out the accepted use and management of the CCTV system and images to ensure the College complies with the Data Protection Act 1998, General Data Protection Regulations, Freedom of Information Act 2000, Protection of Freedoms Act 2012, and Human Rights Act 1998.

The College has produced this policy in line with the Information Commissioner's CCTV Code of Practice.

The College's system comprise several fixed and dome cameras located internally and externally around campuses. All cameras may be monitored and are available for use by approved members of staff. The CCTV system is owned by the College and is subject to annual reviews.

POLICY STANDARDS

1. Purpose of CCTV

The purpose of this policy is to regulate the management and operational use of the CCTV systems.

I. The College has installed a CCTV system to:

- Monitor security of campus buildings.
- Assist in the detection and prevention of crime.
- Assist with the identification, apprehension and prosecution of offenders.
- Assist with the identification of actions/activities that might result in disciplinary proceedings against staff and students.
- Identify and manage vehicle movement around the campuses.

II. The system will be provided and operated in a way that is consistent with an individual's right to privacy.

III. The system will not be used to provide images to the world wide web, record sound or media disclosure.

IV. Covert Recording:

The College has a stock of covert CCTV cameras. Covert cameras may only be used in the following circumstances.

- Reasonable methods have been employed to attempt to resolve the issue.
- Covert processing will be limited and within a reasonable timeframe consistent with the objectives of the deployment.
- Objectives of monitoring must relate to specific suspected illegal, inappropriate or unauthorised activity and be documented in an Impact Assessment.

Written/documented authorisation from the Head of Security will only be given if:

- There is reasonable cause to suspect that illegal activity is taking place or is about to take place or unauthorised activity is taking place that may seriously or substantially affect the operation or reputation of the College.
- That informing the individual(s) in the area to be recorded that recording was taking place would seriously prejudice the objective of making the recording.

The Head of Security will be involved in assessing the need for covert recording in all instances and completing an Impact Assessment for covert CCTV deployment.
The Head of Security, Director of People and Communications and the Chief Financial Officer will decide whether to adopt covert recording, which will be fully documented, and set out how the decision to use covert recording was reached and by whom.

Unless required for evidential purposes or the investigation of crime or otherwise required by law, covertly recorded images will be retained for no longer than 30 days from the date of recording.

2. Owner

I. Cross campus CCTV surveillance systems are owned by United Colleges Group.

II. The Head of Security is responsible for the day-to-day operation of the system as a Data Processor and ensuring compliance with this policy.

III. Contact details:

Head of Security
United Colleges Group,
Paddington Green Campus,
25 Paddington Green, London
W2 1NB
Email: gavin.prime@ucg.ac.uk

3. Overview of system

I. The CCTV system includes approximately 314 fixed and dome PTZ cameras over four campuses. Willesden Campus has 100 fixed cameras, Wembley Campus has 39 fixed cameras, Paddington Campus has 119 fixed & 6 PTZ cameras and Maida Vale has 48 fixed & 2 PTZ cameras.

II. The CCTV system runs 24 hours a day, 7 days a week.

III. The CCTV systems are managed locally across the College estate by the Head of Security and staff from security contractors acting on the College's behalf.

IV. The CCTV system comprises fixed position cameras, pan tilt and zoom cameras, monitors, multiplexers, digital recorders and public information signs.

V. CCTV cameras are located at strategic points on the campuses, principally at the entrance and exit point of sites and buildings, and in main thoroughfares throughout the campuses. All cameras will be prevented from focusing on the frontages or rear areas of private accommodation.

VI. CCTV signage will be prominently placed at strategic points and at entrance and exit points of the campuses to inform staff, students, visitors and members of the public that a CCTV installation is in use.

VII. Although every effort has been made to ensure maximum effectiveness of the CCTV system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

4. Data Protection Act 1998

For the Data Protection Act 1998, United Colleges Group is the data controller.

I. CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act 1998/GDPR. This policy is associated with **UCG's Data Protection Policy**, the provisions of which should be always adhered to. **UCG's Data Protection Policy** is overseen by:

The Chief Financial Officer
United Colleges Group
Paddington Green Campus,
25 Paddington Green, London
W2 1NB
Email: amanda.thorneycroft@cwc.ac.uk

II. The College is required to register its processing of personal data (including CCTV) with the Information Commissioner's Office (ICO). The College's ICO notification registration number is **ZA417156** which is renewed annually in June. The College can be found on the ICO Data Protection Public Register here.

III. Where new cameras are to be installed on the College's estate, Part 4 of the ICO's CCTV Code of Practice will be followed before installation:

- The appropriateness of and reasons for using CCTV will be assessed and documented.
- The purpose of the proposed CCTV system will be established and documented.
- Responsibility for day-to-day compliance with this policy will be established and documented

IV. Consultation with the Chief Financial Officer is required to ensure that the CCTV system is covered by the College's Notification with the Information Commissioner's Office ("ICO").

5. Access to images

I. Access to images will be restricted to those staff that need to have access in accordance with the purpose of the system.

II. Disclosure of recorded material will only be made to third parties in strict accordance with the purpose of the system and is limited to the following:

- Police and other law enforcement agencies where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.
- Prosecution agencies.
- Appropriate members of College staff (such as Human Resources) in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the College's regulations and policies.
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries).

III. Images that have been recorded may be viewed on site by the individual whose image has been captured and/or a uniformed police officer when responding to routine incidents which occurred on the same day. No copies may be taken off site with the exception of release to law enforcement and the Head of Security for internal security training purposes. Please use the form at Appendix A to record the details of these requests.

IV. The Business Development Department have limited and temporary access to external cameras 77 & 78 only at Paddington Campus. Images on these specific cameras cover non-student areas of the on campus rear yard and St Mary's Churchyard (public park) for delivery of SIA PSS Licence training.

6. Individual access rights

I. The Data Protection Act 1998 gives individuals the right to access personal information about themselves, including CCTV images.

II. All requests for access to a copy of CCTV footage by individuals should be made in writing to: GRCI Law Limited, Unit 3 Clive Court, Bartholomews Walk, Cambridgeshire Business Park, Ely, Cambridgeshire CB7 4EA. Email: dpoaas@grcilaw.com Tel: 0333 900 5555

III. The College will respond promptly and at the latest within 30 calendar days of receiving the information to identify the images requested.

IV. If the College cannot comply with the request, the reasons will be documented and the requester will be advised of these in writing, where possible.

7. Access to images by third parties

I. Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under the DPA, and care must be taken when complying with such requests to ensure that neither the DPA, HRA or the CCTV Policy are breached. As noted above, requests from third parties will only be granted if the requestor falls within the following categories:

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry).
- Prosecution agencies.
- Appropriate members of College staff (such as Human Resources) to ensure compliance with the College's regulations and policies.

II. All third-party requests for access to CCTV footage should be made in writing to the named Data Protection Officer in section 6.II. If a law enforcement or prosecution agency is requesting access, they should make a request under Section 29 of the Data Protection Act 1998.

8. Request to prevent processing

I. In addition to rights of access, data subjects also have rights under the DPA to prevent processing (i.e. monitoring and recording CCTV images) likely to cause substantial and unwarranted damage to that person, or prevent automated decision taking (i.e. through the use of visual recognition software) in relation to that person.

II. Should any person visiting United Colleges Group campuses have any concerns regarding the operation of the CCTV systems, the following procedure must be complied with:

- The data subject should be directed to the Head of Security to determine whether the data subject's complaint can be resolved locally. If the Head of Security determines that the data subject is instead making a subject access request or that the data subject is not satisfied, the procedure set out in Section 6 above will be followed.

9. Retention and disposal

I. Refer to **UCG's Data Retention Policy**

II. Unless required for evidential purposes or the investigation of crime or otherwise required by law, recorded images will be retained for no longer than 30 days from the date of recording. Current systems overwrite images on a monthly basis, for example, images on the 5th June begin to be overwritten on the 5th July.

III. At the end of their useful life all images on discs will be erased and securely disposed of as confidential waste. All still photographs and hard copy prints also will be securely disposed of as confidential waste.

IV. Images no longer under investigation may be kept for a period of time for internal training purposes.

10. Maintenance and review

I. This Policy will be reviewed six months after it is agreed or on system upgrade, and thereafter not less than once a year or when the law changes.

11. Complaints regarding operation of system

Complaints regarding the CCTV system and its operation must be made in writing to:

GRCI Law Limited
Unit 3 Clive Court,
Bartholomews Walk Cambridgeshire Business Park,
Ely
Cambridgeshire
CB7 4EA
Email: dpoaas@grcilaw.com
Phone: 0333 900 5555

RESPONSIBILITIES

I. The United Colleges Group Corporation are responsible for:

- Approving this policy.
- Nominating and authorising a Data Controller.

II. The Chief Financial Officer as the Data Controller is responsible for:

- Ensuring that the registration with the Information Commissioner of the College's data control operations is kept up to date and reviewed at least annually.
- Making arrangements for relevant codes of practice issued by the Information Commissioner and other national bodies to be implemented.
- Ensuring that the arrangements for dealing with subject access requests are satisfied.
- Dealing with 'non-standard' subject access requests and act as a final arbiter in sensitive cases.
- Authorising monitoring only in justifiable circumstances, and then only after arranging for an impact assessment to be made and workers and students having been advised that monitoring may be undertaken.
- Reviewing monitoring on a yearly basis to ensure that monitoring is justifiable.

III. Nominated Data Processors:

- Director of Business Intelligence - Student Data Nominated Data Controller
- Head of Security - CCTV processing & monitoring
- Security Contractors (ICTS) – CCTV maintenance, processing and monitoring

LEGISLATIVE FRAMEWORK

Data Protection Act 1998 - Human Rights Act 1998 - Regulation of Investigatory Powers Act 2000

ICO Data Protection Register

LINKS TO OTHER GUIDANCE

Home Office – Surveillance Camera Code of Conduct - Installing CCTV? Things you need to do first | ICO