



CCTV Policy

INTRODUCTION

1. The College has a Closed Circuit Television (CCTV) Surveillance system in the London campus, situated in Devon House. 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 Information Commissioner's Office (ICO) CCTV Code of Practice.
2. The College will comply with 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.
3. CCTV outside of the College campus (including Landlord communal areas inside of Devon House, around the marina etc.) are not the responsibility of the College and are not covered by this policy.

CCTV SYSTEM OVERVIEW

4. The CCTV system is owned by NCH at Northeastern Limited ('NCHNL') and is managed by the College and its appointed contractor. Under current data protection legislation NCHNL is the 'data controller' for the images produced by the CCTV system. The College is registered with the Information Commissioner's Office and the registration number is Z2735495. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's guidance, and is subject to a Data Protection Impact Assessment and a Privacy Assessment.
5. The Director of Resourcing and Operations is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.
6. The CCTV system operates video-only (no audio) cameras across the College's demise, including social, academic, and administrative areas. In total the College will have approximately 22 CCTV cameras across the campus. The cameras are typically placed at access/egress points, stairwells, corridors, and general use areas. **CCTV is not placed inside of classrooms, bathrooms, wellness rooms, or private offices.**

7. A sign is placed at the main College entrance, and other conspicuous locations, in order to inform staff, students, visitors and members of the public that CCTV is in operation.
8. The principal purposes of the CCTV system are as follows:
 - 8.1. Proactive deterrent to crime, particularly those that might involve harm to an individual or the theft or destruction of property.
 - 8.2. Real-time monitoring in the event of an active emergency or major event.
 - 8.3. An investigative tool.
9. There is no facial recognition software, it is used as a tool to keep our community safe, and not as a tracking tool.

MONITORING AND RECORDING

10. Cameras are monitored on a secure device that is in the possession of the Security Staff who maintain day to day security of the campus. Outside of Security Staff hours the device is kept in lockable storage on campus. Images are stored locally on servers located securely in the IT Communication Room.
11. Generally, the video footage is stored locally on the London campus.
12. Designated individuals at Northeastern University's Police Department (NUPD) and Office of General Counsel, both located in Boston, Massachusetts, United States are able to access this video from the United States, for the purpose of advising on an investigation, or advising on other legal or security matters. Northeastern University has a data sharing agreement with the College, and treats all data in accordance with the GDPR and Data Protection Act.
13. The Director of Resourcing and Operations (or their nominated deputy) and Facilities will be the only university personnel on site authorised to download, edit, and distribute video footage for the London campus.
14. The cameras record 24/7, all days of the year. The cameras are not monitored live 24/7. There may be exceptions to this, particularly high threat areas or live event coverage.
15. The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are routinely checked to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.
16. All images recorded by the CCTV System remain the property and copyright of the College.

COMPLIANCE WITH DATA PROTECTION LEGISLATION

17. In its administration of its CCTV system, the College complies with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. Due regard is given to the data protection principles embodied in GDPR. These principles require that personal data shall be:
 - 17.1. Processed lawfully, fairly and in a transparent manner.

- 17.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- 17.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 17.4. Accurate and, where necessary, kept up to date.
- 17.5. 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.
- 17.6. 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. The college ensures it is responsible for, and able to demonstrate compliance with gdpr.

APPLICATIONS FOR DISCLOSURE OF IMAGES

APPLICATIONS BY INDIVIDUAL DATA SUBJECTS

18. For requests by individual data subjects for images relating to themselves, a "Subject Access Request" should be submitted in accordance with the College's Data Protection policy.
19. In order to locate the images on the College's system, sufficient detail as to the time and location must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified. Where a request is excessively burdensome, or unreasonable, the College will notify the requestor, and work in good faith to refine the request.
 - Example 1. A request for "all video from all CCTV for the last week" does not provide sufficient detail to locate the data subject, and is excessively burdensome (as it would require an individual to view hours of video trying to locate the subject)
 - Example 2. A request for "video from the lobby camera, on the first of July, between 1400 and 1600 would provide sufficient detail to locate the data subject.
20. Where the College is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.`

ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

21. A request for images made by a third party should be made in writing to the Director of Resourcing and Operations.
22. In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the

prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation.

23. Such disclosures will be made at the discretion of the Director of Resourcing and Operations, with reference to relevant legislation and where necessary, following advice from the College's Data Protection Officer.
24. Where an allegation of misconduct arises and at the formal request of the HR Manager, the Director of Resourcing and Operations (or their nominated deputy) may provide access to CCTV images for use in staff disciplinary cases.
25. The Director of Resourcing (or their nominated deputy) may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student disciplinary cases.
26. 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 the disclosure.

RETENTION OF IMAGES

27. Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point. Systematic checks of the system retainment will be undertaken by the Security Staff or the College's appointed contractor.
28. Where an image is required to be held in excess of the retention period, the Director of Resourcing and Operations (or their nominated deputy), will be responsible for authorising such a request. All requests must be in writing.
29. Images held in excess of their retention period will be reviewed on a three monthly basis and any not required for evidential purposes or as required by law will be deleted.
30. Access to retained CCTV images is restricted to the Director of Resourcing and Operations (or their nominated deputy) and other persons as required and as authorised.

MONITORING COMPLIANCE

31. All staff involved in the operation of the College's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.
32. All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training and will be required to undertake training in the operation of the CCTV system.

MISUSE

33. All staff who use the CCTV system are required to do so in compliance with this policy and relevant legislation, any staff members who fail to do so will be subject to staff disciplinary proceedings.

Title: CCTV Policy					
Approved by: Executive Committee					
Version number	Date approved	Date published	Owner	Location	Proposed next review date
1.0	September 2021	September 2021	Director of Resourcing and Operations	Academic Handbook/ Policies and Procedures / General / Operations	September 2023
Referenced documents					
External Reference Point(s)					
