University of Nottingham
UK | CHINA | MALAYSIA

CCTV Policy

Stuart Croy
Head of Security Services

July 2023

University of Nottingham
UK | CHINA | MALAYSIA

Contents

1. Introduction

1.1 The University of Nottingham “the University” has in place a CCTV surveillance system “the CCTV system” across its UK campuses. This policy details the purpose, use and management of the CCTV system at the University and details the procedures to be followed in order to ensure that the University complies with relevant legislation and the current Information Commissioner’s Office Code of Practice.

1.2 The University will have due regard to the Data Protection Act 1998, 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 University will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

1.3 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").

1.4 This policy and the procedures therein detailed, applies to all of the University's CCTV systems including Automatic Number Plate Recognition ("ANPR") Licence Plate Recognition Cameras ("LPR"), 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.

2. CCTV System overview

2.1 The CCTV system is owned by the University of Nottingham, University Park, Nottingham, NG2 2RD and managed by the University and its appointed agents. Under the Data Protection Act 1998 the University of Nottingham is the 'data controller' for the images produced by the CCTV system. The University is registered with the Information Commissioner's Office and the registration number is Z5654762. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's Guidance.

2.2 The Head of Security 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.

2.3 The CCTV system operates across the University's academic, administrative and residential sites. Details of the number of cameras can be found at: https://www.nottingham.ac.uk/estates/security/home.aspx

2.4 Signs are placed at all pedestrian and vehicular entrances in order to inform staff, students, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by the University of Nottingham and a 24 hour contact number for the Security Control Centre is provided.

2.5 The Head of Security is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

2.6 Cameras are sited to ensure that they cover University premises as far as is possible. Cameras are installed throughout the University's sites including roadways, car parks, buildings, residential accommodation, licensed premises,

[1] https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

within buildings and externally in vulnerable public facing areas.

2.7 Cameras are not sited to focus on private residential areas and cameras situated in University residential accommodation focus on entrances and communal areas. Where cameras overlook residential areas, privacy screens will be fitted.

2.8 The CCTV system is operational and is capable of being monitored for 24 hours a day, every day of the year.

2.9 Any proposed new CCTV installation is subject to a Privacy Impact Assessment.

2.10 Further information regarding the number and location of CCTV cameras is available at:
https://www.nottingham.ac.uk/estates/documents/security/cctv-installations.pdf

3. Purposes of the CCTV system

3.1 The principal purposes of the University's CCTV system are as follows:
- for the prevention, reduction, detection and investigation of crime and other incidents;
- to ensure the safety of staff, students and visitors;
- to assist in the investigation of suspected breaches of University regulations by staff or students; and
- the monitoring and enforcement of traffic related matters.

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

3.3 The University seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

4. Monitoring and Recording

4.1 Cameras are monitored in the Security Control Room, which is a secure area, staffed 24 hours a day. The Control Room is equipped with a Home Office 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.

4.2 Images are recorded centrally on servers located securely in the University of Nottingham Data Centre and are viewable in Security Service areas by all Security staff. Additional staff may be authorised by the Head of Security to monitor cameras sited within their own areas of responsibility on a view only basis.

4.3 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 and that the date and time stamp recorded on the images is accurate.

4.4 All images recorded by the CCTV System remain the property and copyright of the University.

4.5 The monitoring of staff activities will be carried out in accordance with Part 3 of the Employment Practices Code.[2]

4.6 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 Head of Security will be sought before the installation of any covert cameras. The Head of Security should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert recording.

4.7 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.

4.8 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.

4.9 Security staff wearing body worn cameras will disclose, when approaching persons, that they are being video and audio recorded.

[2] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

5. Compliance with Data Protection Legislation

5.1 In its administration of its CCTV system, the University complies with the Data Protection Act 1998. Due regard is given to the data protection principles embodied in the Data Protection Act. These principles require that personal data shall be:

a) processed fairly and lawfully;

b) held only for specified purposes and not used or disclosed in any way incompatible with those purposes;

c) adequate, relevant and not excessive;

d) accurate and kept up to date;

e) kept for no longer than necessary for the particular purpose;

f) processed in accordance with the rights of individuals;

g) kept secure; and

h) not be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection.

5.2 From 25 May 2018, the University will also comply with the General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be:

a) processed lawfully, fairly and in a transparent manner;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) 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;

and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

6. Applications for disclosure of images

Applications by individual data subjects

6.1 Requests by individual data subjects for images relating to themselves "Subject Access Request" should be submitted in writing to the University's Governance and Information Compliance Team together with proof of identification. Further details of this process are detailed on the University's Governance webpage: http://www.nottingham.ac.uk/governance/records-and-information-management/data-protection/data-protection.aspx

6.2 In order to locate the images on the University's system, 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.

6.3 Where the University 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

6.4 A request for images made by a third party should be made in writing to the Head of Security.

6.5 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.

6.6 Such disclosures will be made at the discretion of the Head of Security, with reference to relevant legislation and where necessary, following advice from the University's Governance and Information Compliance Team.

6.7 Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/Advisor, the Head of Security may provide access to CCTV images for use in staff disciplinary cases.

6.8 The Head of Security may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student discipline cases.

6.9 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.

7. Retention of images

7.1 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.

7.2 Where an image is required to be held in excess of the retention period referred to in 7.1, the Head of Security or their nominated deputy, will be responsible for authorising such a request.

7.3 Images held in excess of their retention period will be reviewed on a three monthly basis and any not required for evidential purposes will be deleted.

7.4 Access to retained CCTV images is restricted to the Head of Security and other persons as required and as authorised by the Head of Security.

8. Complaints procedure

8.1 Complaints concerning the University's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Head of Security at: security@nottingham.ac.uk .

8.2 All appeals against the decision of the Head of Security should be made in writing to the Registrar at registrars@nottingham.ac.uk .

9. Monitoring Compliance

9.1 All staff involved in the operation of the University'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.

9.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

10. Policy review

10.1 The University's usage of CCTV and the content of this policy shall be reviewed annually by the Head of Security with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.