CCTV Policy

Estates Department

June 2023

Document Summary	
Author, Title and Department	**Approving Body**
Facilities Security Manager - Estates	Information Governance Steering Group and Senior Leadership Team
Date of Approval	**Date for Review**
14/09/2020	13/09/2021
	12/06/2024

Revision History			
Version	**Date**	**Author(s)**	**Note**
1.0	09/09/2020	L Jones, R Ward	First issue for SLT approval
1.1	12/06/2023	L Jones	Minor amendment on review

University of Lincoln CCTV Policy

Contents

1. Introduction

1.1 The University of Lincoln “the University” has in place a CCTV surveillance system “the CCTV system” across all campuses and external accommodation facilities. 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 CCTV Code of Practice.

1.2 The University will have due regard to 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. 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’ (“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 Lincoln, Campus Way, Brayford Pool, Lincoln, LN6 7TS and managed by the University and its appointed agents. Under current data protection legislation, the University of Lincoln 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 Z7846984. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner’s guidance.

2.2 The Facilities Security Manager 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: http://estates.lincoln.ac.uk/cctv/

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 Lincoln and a 24-hour contact number for the Brayford Security Control Room is provided.

2.5 The Facilities Security Manager 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, 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 The CCTV system is subject to a Data Protection Impact Assessment. Any proposed new CCTV installation is subject to a Data Protection Impact Assessment. Any new CCTV Camera installation is subject to a privacy assessment.

2.10 Further information regarding the CCTV system is available at: http://estates.lincoln.ac.uk/cctv/

3. Purposes of the CCTV system

3.1 The principal purposes of the University's CCTV system are as follows:

- 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;

- to assist in health and safety investigations of accidents and incident members of the Health & Safety team;

- to assist in the application and enforcement of the University parking policy, and

- the monitoring and enforcement of wider 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 Security Control Room and are viewable in Security Service areas by nominated Security staff. Additional

staff may be authorised by the Facilities Security Manager 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.[1]

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 Facilities Security Manager will be sought before the installation of any covert cameras. The Facilities Security Manager 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 are 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.

5. Compliance with Data Protection Legislation

5.1 In its administration of its CCTV system, the University 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:

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;

[1] https://ico.org.uk/media/fororganisations/documents/1064/the_employment_practices_code.pdf

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.

The University ensures it is responsible for, and able to demonstrate compliance with GDPR.

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 Information Compliance Team together with proof of identification. Further details of this process may be obtained by contacting compliance@lincoln.ac.uk.

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 Facilities Security Manager.

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 Facilities Security Manager, with reference to relevant legislation and where necessary, following advice from the University's 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 Facilities Security Manager may provide access to CCTV images for use in staff disciplinary cases.

6.8 The Security Facilities Manager may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student discipline cases and health and safety incidents.

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 Facilities Security Manager 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 Facilities Security Manager and other persons as required and as authorised by the Deputy Director of Estates.

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 Facilities Security Manager via: estatessupport@lincoln.ac.uk.

8.2 All appeals against the decision of the Facilities Security Manager should be made in writing to the Deputy Director of Estates.

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 Facilities Security Manager with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.

Appendix 1 Use of Body Worn Cameras

Body worn video cameras will only be used by Campus Security staff and whilst they may be worn at all times, they will only be switched on when determined operationally necessary. This decision will be based on the need to fulfil the purposes of the system.

All incidents which involve the use of body worn video shall be logged in the duty log document, documenting the date, time, reason for use, name of authoriser and name of the Security Officer wearing the body worn video.

The Security Officer wearing the body worn video is always responsible for its use. Once recording has commenced the officer should alert those present that the recording will be taking place, stating the following:

- that recording is taking place;
- that it includes audio recording;
- their own name and that of any colleagues;
- the date;
- the time;
- the location; and
- the nature of the incident.

If the recording has started prior to the arrival of the officer at the scene, they must state this upon arrival. Where this is not operationally possible, this information should be provided as soon as it is practicable to do so. Security Officers will also start recording if requested to do so by persons involved in any incident.

Retention of Images
Where camera footage is obtained, it will be retained only for as long as it strictly necessary and for no more than 30 days (unless it is required to support an active investigation, or complaint).

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

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes 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
- Relevant legal representatives
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries)
- Members of staff involved with the University staff and student disciplinary or accident/incident investigation process

Information to statutory prosecuting authorities will require the necessary approval.

All requests for disclosure will be documented and if disclosure is denied, the reason will be recorded.

Individuals' Access Rights
The Data Protection Act 2018 gives individuals the right to access personal information about themselves, this includes CCTV footage and images.

All requests for access by individuals should be made in writing to the University's Information Compliance Team.

Requests for access to body worn camera images must include:

- The date and time the images were recorded
- The location of the incident
- Further information to identify the individual, if necessary

The University will respond promptly and at the latest within 30 days of receiving sufficient information to identify the images requested. If the University cannot comply with the request, the reasons will be documented and the requester advised in writing. Those reasons might include the presence of other individuals in the footage, whose privacy might be infringed by releasing the requested data.