Loughborough University CCTV Code of Practice

1. Introduction

1.1 The CCTV Code of Practice (the Code) seeks to ensure that the Close Circuit Television (CCTV) system used at Loughborough University (the University) is operated in compliance with the law pertaining to data protection. This is currently the General Data Protection Regulation ("GDPR"), Data Protection Act 2018 ("DPA 2018") and the Regulation of Investigatory Powers Act (2000). It includes the principles governing the processing of personal data as set out in Appendix 1. The University uses CCTV only where it is necessary in pursuit of a legitimate aim or public task, as set out in clause 1.3, and only if it is proportionate to that aim.

1.2 The Code is written in line with guidance issued by the Information Commissioner and the Home Office, which can be found at the following websites:

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

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

1.3 The security and safety of all students, staff, visitors, contractors, property and premises is of paramount importance and the University seeks to ensure this as far as is reasonably practicable. The University therefore utilises CCTV:

- To promote a safe environment and monitor the safety and security of its premises;
- To assist in the prevention, investigation and detection of crime;
- To assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings;
- To assist in the investigation of breaches of its Codes of Conduct and policies by staff, students and contractors and, where relevant and appropriate, investigate complaints;
- To provide emergency services assistance;
- To assist with health and safety issues by detecting potential hazards;
- For the performance of a task carried-out in the public interest or in the exercise of official authority in the controller.

1.4 The Code will be reviewed periodically by the Head of Security in conjunction with Human Resources to ensure continued compliance with section 1.1 and 1.2.

2. Scope

2.1 The Code applies to all employees and students of the University, as well as contractors and other persons who may be present, for whatever reason, on University property.

2.2 The Code applies to CCTV systems (including Indigo Vision software) in all parts of the University's campuses.

2.3 The Code does not apply to any Webcam systems located in meeting rooms or lecture theatres operated by Schools or IT, which are used for the purposes of ReVIEW, the

University's lecture capture system. The policy relating to the use of this system can be found at:

https://www.lboro.ac.uk/media/wwwlboroacuk/external/content/services/cap/review/documentsandfiles/Loughborough%20University_Teaching%20Event%20Capture%20Policy_Approved%20Mar18.pdf

3. Roles and responsibilities

3.1 The Chief Operating Officer has the overall responsibility for the Code and has delegated day-to-day responsibility for overseeing its implementation to the post holders identified herein. All relevant staff have been made aware of the Code and have received appropriate training.

3.2 The Head of Security and Director of Estates and Facilities Management are responsible for ensuring that the CCTV system, including camera specifications for new installations, complies with the law and guidance detailed in sections 1.1 and 1.2 of the Code. Where new surveillance systems are proposed to monitor a publicly accessible space on a large scale, the University's Head of Security will conduct a Data Protection Impact Assessment.

3.3 The University hold a list of persons authorised to view CCTV images. All authorised persons are fully trained in the operation of the CCTV system.

3.4 The Director of Human Resources and Organisational Development is responsible for the evaluation and authorisation of locations where live CCTV images are available for viewing via Indigo Vision software.

3.5 Changes in the use of the University's CCTV system can only be implemented in consultation with the University's Information Governance Sub-Committee before being ratified by the Information and Technology Governance Committee, if the changes impact on the processing of personal data. A change in use would be the purposes for which the system is used. For example, proposing to utilise the images captured for research purposes would be a change of use, whereas changing the angle of cameras would not.

4. System description

4.1 The CCTV systems installed in and around the University's campuses cover building entrances, car parks, perimeters, other external areas such as public squares, internal areas such as social/communal spaces, computer rooms, rooms with high value equipment, corridors and reception areas. They continuously record activities in these areas.

4.2 CCTV cameras are not installed in areas that individuals would have an expectation of privacy such as toilets, changing facilities etc.

4.3 CCTV cameras are installed so that they are not hidden from view. Signs are prominently displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area monitored by CCTV. The signs also contain contact details and a statement of the purposes for which CCTV is used. Any employee staffing the contact telephone number must be familiar with this

document and the procedures to be followed in the event that a subject access request is received from an individual or third party.

4.4 The University utilises cameras for the operation of the Automated Number Plate Recognition (ANPR) system at its Loughborough campus. The purpose of the system is to allow entry to and exit from the campus for staff at automated barriers and to inform the University's travel plan. The cameras used for this purpose record vehicle registration data only. The system owner is the Head of Campus Services and it is monitored and operated on a daily basis by Security.

5. Covert surveillance

5.1 Covert recordings (i.e. recordings that take place without an individual's knowledge) may only be undertaken in exceptional circumstances. For example, to prevent or detect an unlawful act or serious misconduct. It should be a proportionate response to what the University is seeking to prevent and only in the absence of other reasonable, less intrusive means of achieving this purpose in accordance with the Regulation of Investigatory powers Act (2000).

5.2 Such recordings may not be undertaken without the prior authorisation of the Chief Operating Officer or, in their absence, the Director of Human Resources and Organisational Development. A rationale will initially need to be submitted by the Dean of the School/Director of Professional Service or, in their absence, their deputy or nominated person. This person will then liaise with the Chief Operating Officer/Director of Human Resources and Organisational Development to make a decision on the suitability and proportionality of such action. All decisions to engage in covert recording will then be documented, along with the reasons.

5.3 Surveillance of this type will only focus on the suspected unlawful activity or suspected serious misconduct. Any information which is not relevant will be disregarded and, where possible, deleted except where such recordings highlight other unlawful activity or serious misconduct.

5.4 Covert recording will only be carried out for a limited and reasonable period consistent with the particular purpose of the recording and will not continue after the investigation is completed.

6. Operating standards

6.1 The operation of the CCTV system will be conducted in accordance with the Code.

6.2 The CCTV system is operated from the Security Control Room (the Control Room). This is a self-contained and secure room, which is staffed 24 hours a day by members of the security team. Monitors are not visible from outside the Control Room. No unauthorised access to the Control Room will be permitted at any time. Other than designated security staff members, trained in their duties, access to the control room will be limited to:

- Persons specifically authorised by the Head of Security;
- Maintenance engineers;
- Members of the emergency services where appropriate; and
- Any other person with statutory powers of entry.

6.3 Before permitting access to the Control Room, security staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. All visitors are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of entry to and exit from the Control Room. A log of shall be retained setting out the following:

- Person reviewing recorded footage;
- Time, date and location of footage being reviewed; and
- The reason for reviewing the recordings.

6.4 CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops via Indigo Vision software, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

6.5 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended. The standards to be met in line with the Codes of Practice referred to in section 1.2 of this Code are set out below:

- Recording features such as the location of the camera and/or date and time reference must be accurate and maintained;
- Cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established; and
- Consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;
- Cameras must be properly maintained and serviced to ensure that clear images are recorded and a log of all maintenance activities kept; and
- As far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

6.6 CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV system which overwrites historical data in chronological order to produce an approximate 30 day/calendar month rotation in data retention.

6.7 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period. Images captured and retained as part of a disciplinary process will be erased at the end of the specified retention period.

6.8 All retained CCTV images will be stored securely and in accordance with data protection legal requirements.

7. Data Subject Rights

7.1 Recorded images, if sufficiently clear, are considered to be the personal data of the individuals (Data Subjects) whose images have been recorded by the CCTV system.

7.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

7.3 Data Subjects can exercise their rights by submitting a request in writing to the Assistant Registrar (Student Office) including evidence of their identity. This can be done in writing or by completing the form which is located at:

https://www.lboro.ac.uk/admin/ar/policy/dpact/procsar/index.htm.

7.4 On receipt of the request, the Data Protection Team will liaise with the Head of Security regarding compliance with the request and they will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

8. Third Party Access

8.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:

- Legal representative of the Data Subject;
- Law enforcement or other statutory agencies including the Police and Social Services;
- Disclosure required by law or made in connection with legal proceedings; and
- HR staff responsible for employees and university administrative staff responsible for students in disciplinary and complaints investigations and related proceedings, after express permission has been granted by the Director of Human Resources and Organisational Development for the former and the Academic Registrar for the latter.

8.2 Legal representatives of the Data Subjects are required to submit to the University a letter of authority to act on behalf of the Data Subject together with the evidence of the Data Subject's identity and their request.

8.3 The Data Protection Team will disclose recorded images to law enforcement and other statutory agencies including the Police once in possession of a form certifying that the images are required for either: an investigation concerning national security; the prevention or detection of crime; or the apprehension or prosecution of offenders; other statutory requirement and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

8.4 All disclosures of CCTV images are recorded in the CCTV Operating Log Book and contains:

- The name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording;
- Brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this Code;
- The crime reference number where relevant; and
- Date and time the images were handed over to the police or other body/ agency.

Any individual/body to whom CCTV images are released will be required to sign an agreement to the effect that the information will only be used for the purposes set out in their request and that it will be disposed of in a safe and secure way once it is no longer required for that purpose.

8.5 Requests for CCTV images for staff or student disciplinary purposes (or complaints purposes) must be authorised by the Director of Human Resources and Organisational Development or the Academic Registrar respectively and by the Head of Security in consultation with the Information Governance Manager.

8.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that legislation.

9. Complaints Procedure

9.1 Any complaints relating to the CCTV system should be directed to the Head of Security promptly and in any event, within 30 days/a calendar month (in line with the retention period) of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office.

9.2 Any complaint regarding an individuals personal data and the way it has been processed (for example, unauthorised access or unlawful disclosure) using CCTV or other surveillance systems will be managed in accordance with the GDPR.

9.3 If a complainant is not satisfied with the response, they may appeal to the Chief Operating Officer. If the complaint is in relation to the processing of personal information, they may also make a complaint directly to the Information Commissioner's Office by writing to:

ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF.

Appendix 1

Principles relating to the processing of personal data under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; and

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.