Loughborough University

Corporate Services

CCTV Code of Practice

1. Introduction

This Code of Practice aims to ensure that the CCTV systems Installed and operated by Loughborough University comply with the law and that the scope, purpose and use of the systems are clearly defined.

2. Definitions

For the purpose of the Code of Practice the following definitions will apply:

- "University" refers to Loughborough University.
- "CCTV" is Closed Circuit Television System.
- "Security Services" refers to Loughborough University Security.
- "Data Controller" is Loughborough University

3. Scope

This Code of Practice is binding on all employees and students of LU University and all employees of contracted out services. It also applies to all other persons who maybe present, for whatever reason, on LU University property.

4. Ownership and Operation

The CCTV system is operated by Loughborough Security whose personnel are employed directly by the University.
The CCTV system, all recorded material and copyright are owned by the University.

5. Principles

The following principles will govern the operation of the CCTV system.

- The CCTV system will be operated fairly and lawfully and only for the purposes authorised by the University.
- The CCTV system will be operated with due regard for privacy of the individual.

- Any changes to the purposes for which the CCTV system is operated will require the prior approval of the Head of Corporate Services and will be published in advance.

6. Purpose of the CCTV System

The system is intended to provide an increased level of security in the University environment for the benefit of those who study, work, live in or visit the campus.

The CCTV system will be used to respond to the following key objectives, which will be subject to annual assessment by use of statistics.

- To detect, prevent or reduce the incidence of crime.
- To prevent and respond effectively to all forms of harassment and public disorder.
- To improve communications and the operational response of security patrols.
- To reduce the fear of crime and create a safer community.
- To gather evidence by a fair and accountable method.
- To provide emergency services assistance.
- To assist with health and safety issues by detecting potential incidents.
- Facilitate the ability to:
  - The identification, apprehension and prosecution of offenders in relation to crime and public order.
  - The identification of any activities/events which might warrant disciplinary proceedings being taken against students or staff.
  - Providing evidence to appropriate people who are involved in disciplinary investigations.
  - The movement of vehicles on campus.

As community confidence in the system is essential, all cameras will be operational. An appropriate maintenance programme is established.

7. System Details

The CCTV system consists of cameras situated on University property, which continuously record activities in that area. The control room is staffed 24 hours a day by members of Security.

8. Installation and Signage

Cameras shall be installed in such a manner as not to overlook private domestic areas. Cameras shall not be hidden from view and signs will be prominently displayed in the locality of the cameras. The signs will indicate:

- The presence of monitoring and recording.
- The ownership of the system.
- Contact telephone number.

If at any time mobile cameras are employed, their use will also be governed by this Code of Practice and communicated via a Loughborough Notices web message.

9. Data Protection Act 1998

Where images of living, identifiable individuals are deliberately recorded, this is likely to comprise those individuals' personal data. The collection, use and storage of personal data are governed by the Data Protection Act 1998. The University is registered with the Commissioner as a Data Controller operating CCTV.

Given that any particular sequence of CCTV recording may include personal data, all such recordings will be treated in accordance with the Data Protection Principles set out in the appendix.

Data subjects' rights, including a right of access to their personal data, (in accordance with Section 7 of the Data protection Act), will be respected where recordings are confirmed to comprise personal data. Where an individual requests access to recordings believed to be their personal data, the matter shall be referred to the data Protection Officer (DP@lboro.ac.uk).

10. Access to Live Footage and Recordings

Access to Live Footage Images captured by the system will be monitored in the Security Control Room which is a self-contained secure room. For operational purposes, and in accordance with the stated purposes of the system, only designated Security staff, trained in their duties, shall have access to live CCTV footage.

Non-essential access to the CCTV Control Room is monitored/controlled and all staff are trained in their responsibilities in respect of the use of CCTV.

Live images may be viewed at any time by the police, however the police do not have the power to record the images or to re-position or focus the cameras directly.

Access to Recordings For operational purposes and in accordance with the stated purposes of the system, only designated Security staff shall have primary access to CCTV recordings. Access may be granted to the police (see below) if appropriate and the requisite data release form is completed.

The Security Manager or nominee may permit the viewing of the CCTV recorded materials by other University staff where this is necessary in connection with the prevention of crime, assisting in the apprehension and prosecution of offenders or matters of national security.

Where University staff requires access to CCTV recorded materials for any other purpose, the matter shall be referred to the Security Manager and the Data Protection Officer.

Disclosure of Recorded Material As the main purpose of the CCTV system is to prevent crime and assist in the apprehension and prosecution of offenders, designated Security staff may release CCTV recorded materials to the police where the University has initiated contact with the police and there is a reasonable belief that the CCTV recorded materials will be of assistance.

Where the police or other official body with prosecuting powers approach the University and request access to CCTV recorded materials they shall be asked to provide appropriate documentation confirming that the information is necessary for either the prevention of crime or the apprehension or prosecution of offenders, or matters of national security. Additionally, the University DPO must be informed of all disclosures and keep a log of them.

Where any other person requests access to CCTV recorded materials, this request shall be forwarded to the Data Protection Officer.

In all cases where recorded materials are disclosed outside the University, the appropriate Security Officer shall ensure that the disclosure is logged and duly signed for.

11. Retention of Recorded Materials and Disposal

CCTV recordings and other materials produced from them shall be retained for a maximum of 30 days/one calendar month unless an incident is recorded which requires further investigation either by Security, the police or another external body with prosecuting powers.

In the latter case, recordings shall be kept for a period of three years from the date of recording.

All media that are no longer required, on which recordings were made will be shredded (in the case of CD/DVD discs) and the appropriate details entered in the Destruction Records.

12. Breaches of Recorded Materials and Disposal

A copy of this Code of Practice will be made available to anyone requesting it. Any complaint concerning misuse of the system will be treated seriously and investigated by the Security Manager or nominee with advice from the Data Protection Officer.

The Security manager or nominee will ensure that every complaint is acknowledged in writing within seven working days, which will include advice to the complainant of the enquiry procedure to be undertaken.

Breaches of this Code of Practice shall be dealt with in accordance with the appropriate disciplinary policy as set out in Ordinance XVII 3 (a). Serious breaches of the Code may result in criminal liability on behalf of the individual which may also be considered as gross misconduct.

Where appropriate, the police will be asked to investigate any matter relating to the CCTV system which is deemed to be of a criminal nature.

Appendix

Data Protection Principles

Processing shall be taken to mean all operations including obtaining, recording, storing, analysing or converting into other formats.

1. Personal data shall be processed fairly and lawfully (and in accordance with the grounds set out in Schedules 2 and 3 or the Act, as appropriate).

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in a manner incompatible with those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which the data is held.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data shall not be held any longer than is necessary in relation to the stated purposes.
6. Personal data will be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

7. The Data Controller shall take appropriate security measures to prevent unauthorised or accidental access to alteration, disclosure or loss and destruction of personal data.

8. Personal data will not be transferred outside the European Economic Area without ensuring there is an adequate level of protection in relation to the processing of personal data.