UNIVERSITY SURVEILLANCE SYSTEMS

CODE OF PRACTICE

Organisation	Leeds Beckett University
Author(s)	Security Manager
Developed in consultation with	Information Governance
Owner	Estates/CARES – Security Service
Target audience	All users to our campuses and buildings
Sensitivity	Public
Approved by	Information Management and Operations Group
Endorsed by	Director of Estates & Facilities
Effective date	11 May 2022
Review Date	Every 3 years or in the event of legislation changes
Status	Published
External references	ICO Surveillance Code of Practice
Links to other internal policies / procedures	Information Management Framework
Version reference	V1
Version History - summary of changes	Replaces the CCTV Policy and Process 2014 – 2021

Policy Document

CONTENTS

1. **Introduction**

Leeds Beckett University (LBU) operates surveillance systems across its campuses. This code of practice details the purpose, use and management of the CCTV and body worn camera system. The code of practice also confirms the detailed procedure to be followed to ensure that the University (LBU) complies with relevant legislation and the ICO (Information Commissioner's Office) Surveillance Camera Code of Practice.

This code of practice and the procedures apply to all the University's CCTV systems including Automatic Number Plate Recognition (ANPR), body worn cameras, webcams, covert installations and any other system capturing images of identifiable individuals for viewing or recording activities of individuals. Surveillance camera images are monitored and recorded in strict accordance with this policy.

This code of practice is based upon guidance issued by the Information Commissioner's Office.

ICO registration number: Z 6734933

Public Register Link: http://www.ico.org.uk/ESDWebPages/DoSearch

This code of practice applies to all employees and students at Leeds Beckett University. This code does not apply to standalone webcams or cameras that will be used solely for teaching and research and requests to use such cameras should be sent to the Information Governance Manager after completing a DPIA.

2. **CCTV system overview**

The CCTV system is owned by:

Leeds Beckett University
Headingley Campus
Beckett Park
Churchwood Avenue
Leeds
LS16 5LF

Under current data protection legislation, the University's Security Manager is the data controller and takes responsibility for the images produced by the CCTV system.

- The University is registered with the Information Commissioner's Office.
- The registration number is Z 6734933.
- The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner's guidance.
- The 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.

The CCTV system operates across the University's academic, administrative and residential sites. Details of the number of cameras can be made available on request.

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

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

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 and licensed premises.

Cameras are sited internally and externally to monitor the campus and to support vulnerable public-facing areas. Cameras are not sited in private residential areas or external spaces outside of our campuses.

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, this will be managed in line with the POFA and guidance from the Information Officer.

- The CCTV system is operational 24 hours a day, 365 days a year.
- The CCTV system is subject to a Data Protection Impact Assessment.
- Any proposed new CCTV installation is subject to a DPIA and Privacy Policy.
- Any cameras which are fitted externally will be for monitoring of space external to the University, however, within our City Campus a number of these cameras do pick up paths and roads near to our buildings. We do not specifically monitor these, however, there may be requests from the Police to access some of this data.

3. Purposes of the CCTV system

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

- the prevention, reduction, detection and investigation of crime and other incidents;
- to assist with health and safety of staff, students and visitors;
- To prevent and respond effectively to all forms of harassment and public disorder
- to assist in formal investigation of suspected breaches of University regulations by staff or students;
- the monitoring and enforcement of traffic related matters;
- The CCTV system will be used to monitor the University's building and campuses to identify incidents which require a response. Any response should be proportionate to the incident being witnessed;
- The University seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy and in accordance with 12 principles covered by the surveillance camera commissioner code of practice;

Cameras are monitored from the Security Control Room, which is a secure area, staffed 24 hours a day. The Control Room is equipped with a radio system and supports security systems, fire and building alarm systems. Within the security team all staff are trained to work in the Control Room and support patrols on campus. These are all uniformed security officers who support the Control Room, provide foot and mobile patrols, respond to incidents and are first responders to emergencies on campus.

There are additional service areas that have the capability to view cameras within their own area. The area can only see cameras live; they cannot review or download information. Any additional system to support cameras being viewed in areas must be authorised by the Security Manager.

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

4. Body Worn Cameras (BWC)

The University will deploy BWCs to University security staff. The camera when operated by the University security officer will capture both video and audio information, which collectively falls under the category of body worn video (BWV). The collection, downloading, storage, sharing and deletion of personal data are described in this section to assist in identifying where risks to privacy, data security and compliance may arise.

In accordance with legislation set out in the Surveillance Camera Code of Practice the use of BWC by Leeds Beckett University staff must be:

- Lawful
- Managed
- Overt
- Proportionate, legitimate and necessary
- Incident specific
- In support of and does not replace conventional forms of evidence collection

Only uniformed security officers trained in the use of BWCs will be deployed with the equipment. They may be deployed in response evidence-based security roles. The BWC unit will be affixed to the front of their uniform, clearly displaying the words 'CCTV' on the camera.

Acting within the above principles, a detailed Standard Operating Procedure (SOP) and training will be provided to the security team, which includes:

- The decision to start and stop recording video and audio will lie with the security officer (user). When officers use the BWC and start recording they will announce that recording is taking place. As recording is incident specific, the cameras will not be permanently recording when being worn by University security officers.
- Any images and sound recorded are held within the camera carried by the security officer up to the point they are downloaded at the end of the incident or their shift.
- Security officers are guided by the SOP regarding the use of the equipment, and this confirms what action should be taken where people object to being recorded, ask for an event to be recorded, and when they should stop recording. Equally, officers may have to justify not recording in any circumstance.
- Any data captured by the BWCs will be handled and stored either on a standalone computer that is situated in a secure and controlled environment, or within a secure drive within the university's network system. Images burnt to disc, or otherwise copied, will only be provided in line with agreed surveillance camera practices.

5. Capture and use of data

5.1 Capture the image

When images are captured, the following details are logged; camera number, position, time, location (read only) and this is reliable and trustworthy data.

5.2 Maintain the data and the image as captured, there is no provision to edit or change the data

The control and management of digital recordings and all discs belong to and remain the property of the University. Disc handling procedures are in place to ensure the integrity of the image information held.

5.3 Storage

CCTV (closed circuit television) images are recorded to DVRs in buildings where we have IP encoded cameras and to central comms rooms at each campus for all NVRs which support our IP cameras. All recording devices are in secure comms rooms with restricted access. BWC recordings are downloaded from a docking station to a secure drive on a secure PC within the security area.

All data on recording devices are viewable in the Security Control Room and restricted to specific PCs in the Control Room and can be viewed, reviewed and downloaded in this area. There are several analogue decoded cameras where data must be downloaded at the recorder by the on-site engineer.

All data is stored for a designated period, with restricted access within the Security Control Room. A log will be maintained of who is accessing the space, the job designated and where access is required.

5.4 Retention schedule

Surveillance images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

Any images downloaded to support police or other investigations will only be retained for 3 months from receiving an information access request and then securely destroyed.

Where an image is required to be held longer than the retention period referred to, the security manager or their nominated deputy will be responsible for authorising such a request.

Images held in excess of their retention period will be reviewed on a 30-day basis and any not required for evidential purposes will be deleted.

Access to retained CCTV/BWC images is restricted to the security manager and other persons as required and as authorised by the security manager.

All images are downloaded onto a CD. 3 copies are downloaded, they are stored within

the Control Room and disposed of by being shredded.

6. Compliance with information legislation

In the administration of its Surveillance System, the University complies with but is not limited to the following legislation:

- UK General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Human Rights Act 1988

For further details on the University process please see:

https://www.leedsbeckett.ac.uk/our-university/public-information/information-compliance/

The University ensures it is responsible for, and able to demonstrate compliance with GDPR principles which stipulates that 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;

f) 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;

7. Applications for disclosure of images

A record of any disclosure made under this policy will be held on the surveillance management log, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

Access to the control room and recorded/live footage will be prohibited except for lawful, proper and sufficient reasons (eg. official visits from law enforcement or inspection agencies, security staff, cleaning staff, etc) and only then with the personal authority (verbal or written) of the University Security Manager. All visitors to the control room will be required to sign the visitor's book.

7.1 Applications by individual data subjects

Requests by individual data subjects for images relating to themselves ("Subject Access Request") should be submitted in accordance with University guidance on the information compliance webpages: https://www.leedsbeckett.ac.uk/our-university/public-information/information-compliance/

In order to locate the images on the University's system, sufficient detail must be provided by the data subject to allow the relevant images to be located and the data subject to be identified.

All access to data requests will be handled in line with the University Access to Information Policy.

7.2 Access to and disclosure of images to third parties or a request made by a third party

All requests should be made in writing to the University. On receipt of any request when received in Security Services, a scanned copy should be sent to the Information Compliance team.

Requests by third parties should be submitted in accordance with University guidance on the information compliance webpages. All access to data requests will be handled in line with University Access to Information Policy and in consideration of the Data Protection Act 2018.

Requests for information by the Police and other authorities must be accompanied by the relevant data protection form duly signed by the appropriate authority and must also be made through the Information Governance Manager. Disclosures in relation to the prevention or detection of crime and the apprehension or prosecution of offenders may occur without the consent of individuals under Schedule 2 Part 1.2 of the Data Protection Act 2018.

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.

8. Monitoring compliance

All staff involved in the operation of the University's surveillance system will be made aware of this policy and will only be authorised to use the surveillance systems in a way that is consistent with the purposes and procedures contained therein.

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

This policy will be published on the University policy webpage and will be disseminated through staff training, information asset owners, and the information management operational group (IMOG)

Any use of the CCTV system or materials produced which is outside this code and is inconsistent with the objectives of the system will be considered gross misconduct. Misuse of the system will not be tolerated; continuing public support is vital. Any person found operating outside these codes without good and reasonable course will be dealt with under the University disciplinary procedure. If any breach constitutes an offence under criminal or civil law then court proceedings may be taken.

Any complaint concerning misuse of the system will be treated seriously and investigated by the Security Manager and Registrar and Secretary's Office. The Security Manager and Registrar and Secretary's Office will ensure that every complaint is acknowledged in writing within seven working days which will include advice to the complainant of the inquiry procedure to be undertaken.
Where appropriate the Police will be asked to investigate any matter recorded by the CCTV system which is deemed to be of a criminal nature.

9. Code of Practice review

The University's usage of CCTV and the content of this code of practice shall be reviewed every 3 years by the security manager with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.