Code of Practice on the Operation of Closed Circuit Television (CCTV)
INDEX

Introduction and Accountability
Complaints
Objectives
The System
The Campus Support Control Room
Campus Support Control Room Administration and Procedures
Monitoring Procedures
Video Tape Procedures
Code of Practice on the Operation of CCTV

The Scope of this Code

Introduction
The University of Liverpool has installed a comprehensive CCTV surveillance system throughout the main campus and also has a number of cameras in other remote locations, such as the Veterinary Field Station at Leahurst and the Botanic Gardens at Ness. Images are monitored from a central control room on the main campus whilst some are monitored and recorded locally. The system is owned by the University of Liverpool and the control room is staffed by Officers from the Campus Support Services Division of Facilities, Residential & Commercial Services (FRCS).

This Code of Practice, which has been agreed with Merseyside Police, has been prepared for the guidance of managers and the operators of the CCTV system and for the information of all members of the University community. It applies to all surveillance systems throughout the University. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the University, consistent with the obligations on the University imposed by the ‘Data Protection Act 1998’/’The General Data Protection Regulation 25th May 2018’.


Accountability and Complaints
The Director of FRCS, Director of Estates Management and Head of Campus Support Services are jointly responsible for the operation of the CCTV system, and in the first instance for ensuring compliance with this Code of Practice. Breaches of the code by control room staff will constitute matters of discipline under the relevant conditions of employment, but it is also recognised that other members of the University may have concerns or complaints in respect of the operation of the system. Any concerns in respect of the system’s use or regarding compliance with this code, should in the first instance be addressed to the Head of Campus Support Services. These rights do not alter the existing rights of members of the University under the relevant grievance or disciplinary procedures.
Contact Numbers:

Director of FRCS 58170
Director of Estates Management 59026
Head of Campus Support Services 43216

1. Objectives

1.1. CCTV has been installed to reduce the fear of crime generally and to provide a safe public environment for the benefit of those who live or work within the University or visit it consistent with respect for individuals’ privacy. These objectives will be achieved by the monitoring of the system, to:

- Assist in the prevention and detection of crime;
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order; and to
- Facilitate the control of car parking and the movement of vehicles.

2. The System

2.1. The system of CCTV surveillance encompasses the Main Campus in the City of Liverpool in addition to the Off-Site Campuses. The system is monitored from a twenty-four hour control room based on the Main Campus and an off-site location.

2.2. The system is operational and images will be monitored for twenty-four hours per day, throughout the whole year.

2.3. Cameras will not be hidden from view and steps will be taken, e.g. by the installation of signage, to inform the public of the presence of the system and its ownership.

2.4. To ensure privacy, the cameras are prevented from focusing or dwelling on the frontages and rear areas of private accommodation and this will be demonstrated on request. Where domestic areas such as gardens or areas not intended to be covered by the scheme border those spaces which are intended to be covered by the equipment, then the Head of Campus Support Services or the Director of Estates Management or nominee, will consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked. The scheme will be operated with a high regard for the privacy of the individual.

2.5. There will be no sound recording from any part of the CCTV system.

2.6. Images captured on camera will be transmitted to a central control room where they will be recorded for use in accordance with this Code of Practice.

2.7. Although every effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.
2.8. For the purpose of the Data Protection Act 1998/The General Data Protection Regulation 25th May 2018, the data controller on behalf of the University of Liverpool, is legally responsible for the management and maintenance of the CCTV system.

2.9. All requests for additional CCTV installations of equipment need to be agreed with the Head of Campus Support Services before any request is sanctioned. Any installation of CCTV equipment without approval from the Head of Campus Support Services, can request the CCTV equipment to be discontinued.

3. The Control Room

3.1. Images captured by the system will be monitored in the control room, a self-contained and secure room on the Main Campus and Off-Site Campus. The monitors cannot be seen from outside of the control room.

3.2. No unauthorised access to the control room will be allowed at any time. Normal access to it will be strictly limited to the duty controllers, authorised staff members and senior management. Police officers may only enter with the explicit consent of the Head of Campus Support or his nominee. A list of University staff authorised for routine access to the control room including senior management, will be compiled and maintained.

3.3. Staff, students and visitors may be authorised to enter the control room on a case-by-case basis. Written authorisation is required and may only be given by the Director of Estates Management or by the Head of Campus Support Services. Each separate visit will require individual authorisation. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may also be granted to persons with a legitimate reason to enter the control room.

3.4. Before granting access to the control room, controllers must satisfy themselves of the identity of any visitor and that visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors’ log, which shall include details of their name, their department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the times of their entry to and exit from the control room. A similar record shall be kept of the controllers on duty in the control room at any given time and of any visitors to the control room in an emergency.

4. Control Room Administration Procedures

4.1. An incident log (CRIM) will be maintained in the control room and kept securely there. Brief details of incidents will be noted in it together with any consequential action taken.

It is recognised that the images obtained comprise personal data and are subject to the law on data protection. All copies will be handled in accordance with the University and police working procedures which are designed to ensure integrity of the system. The Head of Campus Support Services will be responsible for the development of and compliance with the working procedures in the control room. A log will be kept for the purposes of recording the use of the transfer of DVDs, their use and retention for evidential purposes. The transfer of such images to the police and other parties where authorisation has been given and their retention is required for evidential purposes. The identity of the police officer or other person receiving the disc must sign the log.
Recorded images will only be reviewed with the authority of the Head of Campus Support Services or, where it is not reasonably practicable to contact him, his nominee.

Copies of digital messages will only be made for the purposes of crime detection, evidence in relation to matters affecting safety, evidence for hearings or where otherwise required by law.

In order to comply with the objectives of this code relating to public safety, (see paragraph 1.1) control room staff will monitor University car parks giving advice to staff and students through the intercom systems where this is appropriate. Monitoring of car parks will also take place in order to assist colleagues with the enforcement of the University car parking regulations and the prevention and detection of crime.

4.2. Communications

Dedicated image and radio or telephone links with the police control room may be provided in due course. These will be used to relay information on incidents that arise and to communicate information. Camera control and image recording facilities will not be provided for police use in their control room.

Emergency procedures will be used in appropriate cases to call fire brigade or ambulance services.

In addition, liaison with other groups (e.g. Liverpool City Council), will be developed and used as considered appropriate.

4.3. Staff

All staff are aware of the sensitivity of handling CCTV images and recordings. Vetting of control room staff and managers may be carried out by the police.

The Head of Campus Support Services will ensure that all staff, are fully briefed and trained in respect of all functions, both operational and administrative arising within the CCTV control operation. Training in the requirements of the Data Protection Act and this Code of Practice will also be provided.

4.4. Liaison

The Head of Campus Support Services, will meet on a regular basis with the police and other officers in order to continue to develop good practice in the use of CCTV. Other meetings between senior police officers and Senior University staff will take place where it is thought necessary to discuss policy issues in respect of the use of CCTV.

4.5. Recording

The control room system is supported by digital recording facilities which will function throughout the day and night. In addition, incidents can be recorded in ‘real time’ where necessary. The system will be capable of retrieving images to a digital system or to a DVD disc.

Images are automatically stored no longer than 7 days for analogue systems, and no longer that 28 days for I.P. systems.
5. Monitoring Procedures

5.1. Camera Control

One operator, who will be a member of the Campus Support Services staff from FRCS, will be available to work in the control room throughout the twenty-four hour day, 7 days a week. The control room will never be without at least one operative, who will be relieved when refreshment or other breaks are necessary.

5.2. The control of the system will always remain with the University but at the University’s discretion the cameras may be operated in accordance with requests made by the police during an incident to:-

Monitor potential public disorder or other major security situations;

Assist in the detection of crime;

Facilitate the apprehension and prosecution of offenders in relation to crime and public order.

On each occasion the police may obtain assistance with their operations, a report setting out the time, date and detail of the incident will be submitted to the Head of Campus Support Services or, where it is not reasonably practicable to contact him, his nominee details of such incident will be recorded.


6.1. Control and management of tapes and digital recordings

All tapes belong to and remain the property of the University of Liverpool and held for no longer that 7 days. Tape handling procedures are in place to ensure the integrity of the image information held (see Section 6.3).

6.2. Access to recording

Generally, requests for viewing or copying of tapes or obtaining digital recordings will only be granted if they come from the Police, Head of Campus Support Services or nominee. Police requests will arise in a number of ways, including:

(a) Regular requests for a review of recordings, in order to trace incidents that have been reported

(b) Immediate action relating to live incidents e.g. immediate pursuit

(c) For major incidents that occur, when images may have been recorded continuously

(d) Individual police officer seeking to review recorded images within the control room

Requests for access may also be made by individuals to view their own recorded images under the terms of the Data Protection Act 1998/The General Data Protection Regulation from 25th May 2018. Applications for access under the Data Protection Act 1998/The General Data Protection Regulation from 25th May 2018 should be made to the Data Protection Officer and should specify the location, date and time to which the enquiry relates. The application form can be downloaded from the web site http://www.liv.ac.uk/dp/ or is available on request from the Data Protection Officer.
6.3. **Standards**

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the Code reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998. These aspects of the Code reflect the Second and Sixth Data Protection Principles of The General Data Protection Regulation from 25th May 2018. (The reasons for obtaining and recording images via CCTV are set out in paragraph 1.1 of this code under Objectives).

All control room staff should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

Access to recorded images will be restricted to staff who need to have access in order to achieve the purposes of using the equipment.

Disclosure of the recorded images to third parties or to other individuals or departments within the University will be made only in the following limited and prescribed circumstances.

All requests for access or for disclosure will be recorded. Decisions on access to recorded images by persons other than police officers will be made by the Head of Campus Support Services after consultation with the Data Protection Officer. Requests by police for access to images will not normally be denied and can be made without the above authority provided they are accompanied by a written request signed by a police officer. The transfer of such images to the police and other parties where authorisation has been given and their retention is required for evidential purposes. The identity of the police officer or other person receiving the disc must sign the log.

If access or disclosure is denied by the Head of Campus Support Services, the reasons will be documented.

If access to or disclosure of the images is allowed (either by the Head of Campus Support Services in non-police cases or by a member of the control room staff where the proper format has been followed – as above – in police cases), then the following will be documented.

*See also below, at 6.4 ‘Access by Data Subjects’*

Recorded images will not normally be made more widely available – for example they will not be routinely made available to the media or placed on the Internet or University Websites.

If it is intended that images will be made more widely available, that decision will be made by the Head of Campus Support Services or his nominee after consultation with the Data Protection Officer. The reason for the decision will be documented.
6.4. Access by data subjects

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. User of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images.

These aspects of this code reflect the principles of the Data Protection Act 1998/ The General Data Protection Regulation from 25th May 2018.

All control room staff should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

Access to recorded images will be restricted to staff who need to have access in order to achieve the purpose of using the equipment.

All access to the medium in the control room on which the images are recorded will be documented.

Disclosure of the recorded images to third parties or to other individuals or departments within the University will be made only in the following limited and prescribed circumstances.

- Law enforcement agencies where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies
- Relevant legal representatives
- Where it is decided that the public’s assistance is needed to identify a victim, witness or perpetrator in relation to a criminal incident, images from the system will be provided to the media or placed on to the University’s websites. As part of that decision, the wishes of the victim of an incident will, where possible, be taken into account.
- People whose images have been recorded and retained and disclosure is required by virtue of the Data Protection Act 1998/ The General Data Protection Regulation 25th May 2018.

All requests for access or disclosure will be recorded. Decisions on access to recorded images by persons other than police officers will be made by the Head of Campus Support Services and the following will be required.

- Individuals to provide dates and times when they visited University and their location – for example which campus site and specific area or building.
- The individuals will provide two photographs of themselves – one full face on side view with the completed form.
- They will provide to the person receiving the application proof of their own identity e.g. a utility bill, a driving licence or a passport.
- They will be asked whether they would be satisfied with merely viewing the images recorded.
- A written decision on their request will be sent to them within 21 days, or less than a calendar month under The General Data Protection Regulation from 25th May 2018.
6.5. Rights of Data Subjects

The procedure outlined above and the use of data subject form complies with Section 7 of the Data Protection Act 1998 and Article 15 of The General Data Protection Regulation from 25 May 2018 enabling the Head of Campus Support Services or his nominee to inform individuals as to whether or not images have been processed by the CCTV system. The University is not obliged to comply with a request under this section unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the information which that person seeks.

Where the University cannot comply with the request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless the other individual has consented to the disclosure of the information to the person making the request – or – it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

6.6. Continuity of evidence – procedures for tracking tapes (when not using digital recording)

All tapes are marked with a reference number which is prefixed by the letter ‘A’. To ensure that tapes can be used in evidence, the following procedures will be followed (the controller means the person in charge of the recording system whatever its location)

(a) The controller shall register the date and time for tape insert and ejection, including tape reference in the tape log.

(b) If the tape is kept in an archive for evidence purposes the fact that this has been done together with the date, time and tape reference must be noted in the tape log and on the tape.

(c) Any replacement tape must have the same identification reference recorded on it as the archived tape but will be prefixed by the letter ‘B’.

6.7. Continuity of evidence – procedure for identifying digital images

Event logs are automatically created with digital image recordings and searches for incidents can be made by inputting search parameters. Once an image relevant to an incident or criminal investigation has been identified its digital reference will be recorded and a copy made if required either onto a disc or standard VHS video tape. A record will be kept in accordance with paragraph 6.3. The recording will be archived and the disc or tape will be given a reference number before being handed over to a third party. The reference will relate to identifying characters in the archived recording.
6.8. Photographs

Photographs taken from video recordings are subject to the same controls and the same principles of data protection as other data collected in the control room. They may only be obtained to assist the identification, apprehension and prosecution of alleged offenders, during staff training and for other purposes consistent with the purposes of the CCTV system set out in paragraph 1 above. Photographic material may only be produced by control room staff using equipment available in the control room.

Photographs will normally be supplied to the police upon reasonable request. Any requests for viewing photographs other than a police request will be considered by the Head of Campus Support Services in liaison with the Data Protection Officer.

All photographs produced must be recorded along with the identity of the requesting person, date and other appropriate information in the tape log.

6.9. Disposal

All recordings will be subject to a retention policy and kept only for the period required for the purposes outlined above.

Compact disc recordings will be destroyed and disposed of as confidential waste when they are no longer required as evidence. Recordings on the system’s hard disc will be deleted when relevant copies have been made onto DVDs.

Video prints will be retained until they are no longer useful as evidence or have become outdated. Thereafter they will be destroyed and disposed of as confidential waste.

At the end of their useful life all tapes will have their images erased and disposed of as confidential waste.