

## CCTV Code of Practice

### Introduction

The use of Closed Circuit Television at the University of Birmingham has expanded rapidly since 1990, and along with this so has the need for recognised standards and safeguards. There is a need for the University to ensure accountability, along with a good quality; effective and well managed system.

Cameras are installed throughout the campus including car parks, as part of an ongoing programme of installation phased over several years. The CCTV system is monitored and recorded at the security control room. It is wholly owned by the University of Birmingham and is subject to a service and maintenance agreement.

The Code of Practice also applies to schools and departmental CCTV systems

The purpose of the Code of Practice is to set out clear standards so that it complies with the Human Rights Act, 1998 and The Data Protection Act, 1998 to ensure that the system is used professionally by security staff and others.

The University of Birmingham is registered under the Data Protection Act, 1998.

The Code of Practice Principles shall also apply to Webcams where they are placed on University of Birmingham property.

### Objectives

The use of CCTV is designed to provide a safer environment for the staff students and visitors to the campus, whilst reducing the fear of crime generally and is designed to:

- Assist with prevention and detection of crime
- Assist with control and access to car parking
- Aid the identification, apprehension and prosecution of offenders in relation to crime whilst respecting the privacy of the individual.
- Maintaining good order on campus.
- Assist with identification of breaches of University Charter, Statutes, Ordinances and Regulations.

### The System

Currently the system of CCTV surveillance covers much of the Edgbaston campus. It is also intended to encompass all other CCTV images that in due course are added to the system and monitored at the twenty four-hour control room located in the Security Centre on the Edgbaston Campus. The system also includes the ability to use covert cameras from time to time for internal enquiries, where a specific criminal activity has been identified. This will only occur on an exceptional basis.

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

Cameras will not be hidden from view; signs will be erected throughout the campus advising of the presence of the CCTV system and its ownership, save where covert cameras are required for internal enquiries on an exceptional basis, departmental and school systems will comply with the Code of Practice.

## Principles

It is recognised that the images obtained are sensitive and subject to the law on Data Protection.

Images may be recorded in colour or monochrome but with no sound recording.

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. The scheme will be operated with a high regard for the privacy of the individual.

Images captured on camera will be transmitted to the Security Centre Control Room (or School/Department control room) where they will be recorded for use in accordance with this Code of Practice.

Every effort is 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 within the area of coverage.

The system will be maintained and reviewed regularly to ensure that data is accurate and secure.

## The Control Room

Images captured by the system will be monitored in the Security Control Room, a self contained and secure room in the Security Centre. Normal access to the control room is strictly limited to the duty controllers, and personnel authorised by the Security Manager. The monitors cannot be viewed from outside the Control Room.

### Declaration of Confidentiality

Regardless of their status, all authorised visitors to the Control Room will be required to sign the visitor's book 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.

**Note:** Each page of the visitor's book will contain a declaration stating:

*'In signing this visitor's book all visitors to the control room acknowledge that the precise location of the CCTV monitoring room is, and should remain, confidential and that they agree not to divulge any information obtained, overheard or seen during their visit'.*

Consideration may also be given to displaying a notice at the entrance to the room and to include reference to that notice in the declaration by visitors.

## Control Room - Administration and Procedures

- The Security Manager will have responsibility for the Control Room to ensure that the provisions of the Data Protection Act, 1998 are followed.

- An incident log will be maintained in the control room and kept secure. Brief details of incidents will be noted together with any action taken.
- All copies will be handled in accordance with the University procedures designed to ensure the integrity of the system. The Security Manager will be responsible for the development of and compliance with the working procedures in the control room.
- A log will be kept for the purpose of recording the use of tapes, their use by others and retention for evidential purposes and when they are wiped and destroyed.
- Tapes will only be reviewed at the request of the Police or with the authority of the Security Manager or the Assistant Security Manager. Police requests must be submitted in the appropriate form.
- All staff working in the Control Room will be required to complete a declaration, reminding them of the duty of confidentiality and confirming that they have received a copy of the University's Code of Practice.
- No copies of tapes will be made.
- Control room staff may also monitor University 'pay and display' car parking areas, giving advice to staff, students and others through the intercom systems where appropriate. Monitoring of other car parks, including entrances and exits will also take place in order to assist with the management of car parking, and the enforcement of car parking regulations.
- Emergency procedures will be used in appropriate cases to call police, fire or ambulance services

## **Staff**

- All staff will be made aware of the sensitivity of handling CCTV images and recordings.
- The Security Manager 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. Camera installers may also carry out training.
- Training in the requirements of the law on the Data Protection Act, 1998 and Human Rights Act, 1998 will be given to staff who are required to work in the Control Room.

## **Control, Recording and Management of Videotapes**

- All tapes belong to and remain the property of the University of Birmingham. Tape handling procedures are in place to ensure the integrity of the image information held.
- The Control Room system is supported by video tape and digital recording facilities that will function throughout in 'time lapse'. In addition, incidents can be recorded in 'real time' where necessary.
- Each tape will be uniquely identified and all activities relating to each tape, e.g.: date and hours of recording, viewing for specific purposes, tapes retained for evidence, tapes wiped clean and reused will be recorded in the tape log. Digital images are automatically date and time stamped.
- If videotapes are used, they will be changed each day at 04:00 by the officer on duty in the Control Room – details of each change will be recorded in the tape log.

- Tapes will be retained for 31 days from the date of recording, erased then re-used on no more than twelve consecutive occasions. Once a tape has reached its maximum use, its content will be erased prior to disposal. Digital images will be retained for 31 days and will then be deleted.
- In the event of the tape being required for evidence, it will be retained for a period recommended by the Police. In the case of digital images, a copy of the data will be available to the Police and retained as required.

## Access to tapes

- Generally, requests for viewing or copying of tapes will only be granted if they come from the police or the data subject (i.e., the individual who has been recorded). The request should be made in the first instance to the University's Data Protection Officer, who will then liaise with the Security Manager. Police requests may arise in a number of ways:-
  - (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 tapes may be recording continuously.
  - (d) Individual police officer seeking to review tapes within the control room
- Requests for access to tapes from persons other than the Police will be considered on a case by case basis. The Security Manager will consider such requests. Access to tapes in these circumstances will only be granted where that is consistent with the obligations placed on the University by the Data Protection Act, 1998 and the Code of Practice on CCTV issued by the Office of the Information Commissioner from time to time.
- In addition to the Police, third parties who may be required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
  - (i) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
  - (ii) Solicitors
  - (iii) Plaintiffs in civil proceedings
  - (iv) Accused persons or defendants in criminal proceedings
- Upon receipt from a third party of a bona fide request for the release of data, the Security Manager (or representative) should:
  - (i) Not unduly obstruct a third party investigation to verify the existence of relevant data.
  - (ii) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena, (it may be appropriate to impose a time limit on such retention which should be notified at the time of the request).
- Where a request is made by a claimant, accused persons or defendants, the Security Manager (or nominated representative) should:

- (i) Be satisfied that those parties have explored other avenues for securing any evidence that may be contained upon such film footage held by the University. However, this shall not preclude the rule of 'best evidence' and the need to secure it during Police investigations.
- (ii) Treat all such enquiries with strict confidentiality.

## Notes

*The release of data to the police may not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc.*

*Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, should be required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. (It may be considered appropriate to make a charge for this service. In all circumstances data will only be released for lawful and proper purposes).*

*There may be occasions when an enquiry by a claimant, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.*

*The Security Manager or Assistant Security Manager should decide which (if any) "other agencies" might be permitted access to data. Having identified those 'other agencies', such access to data will only be permitted in compliance with this Standard.*

## Viewing and release of tapes

- If a request is made by the data subject, the Police or any other person to view or copy a tape, a record will be made of the request and any subsequent viewing or copying in the tape log, or the reason for the refusal of the request.
- All subject access requests will be dealt with by the University Data Protection Officer. Upon receiving a request she will determine whether disclosure to the individual would entail disclosing images of third parties. If such images are not to be disclosed, arrangements will be made for those images to be disguised or blurred and may engage another party or a company to carry out that type of editing subject to guarantees regarding security measures in relation to the images.
- If tapes are copied or handed over to the Police or other authority, the event will be noted in the log and the details and signature of the recipient obtained. Details in the log must include the name and identification of the person together with the date and time removed and the date and time returned.
- Where a tape is handed over to the Police, the officer making the request must complete the West Midlands Police form WA 170, a copy of which will be kept with the tape log.
- The removal of tapes will normally be permitted only for a fixed period which will be long enough for a third party to view them or - where they may be required for evidence - no longer than a court

may require them. Tapes that may be required by the Police are to be retained securely until it is confirmed that they are not required or no longer required for evidential purposes. Tapes will not be released except in these circumstances.

- All tapes, which have been viewed by third parties or are no longer required for evidence, will have their images erased and returned for use or disposed of as confidential waste.
- All tapes are marked with a reference number and are defined by a prefix letter with a date. To ensure that tapes can be used in evidence, the following procedures will be followed:
  1. The controller should register the date and time of tape insert and ejection, including tape reference in the tape log.
  2. If the tape is kept in archive for evidential 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.
  3. Any replacement tape must have the same identification reference recorded on it as the archived tape, but will be prefixed by the letter 'R'.

## **Photographs and Video Prints**

- Photographs or images 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.
- Photographic material may only be produced by persons authorised by the Security Manager or the Assistant Security Manager.
- Photographs will normally be supplied to the police upon reasonable request. Any request for viewing photographs other than for Police officers will be considered by the Security Manager or the Assistant Security Manager.
- All photographs produced must be recorded along with the identity of the person requesting, together with the date and other appropriate information in the tape log.

## **Disposal**

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

## **Standards and Rights**

- All staff involved in operating the CCTV equipment will be trained to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage to that individual. They will refer such requests to the University Data Protection Officer, the Security Manager or the Assistant Security Manager.
- The individual making such a request will be provided with a written response within 21 days setting out their decision.

- If the University's Data Protection Officer or other designated member of staff decides that the request will not be complied with, they must set out their reasons in the response to the individual.
- If within 21 days of that notification, the individual requires, in writing, the decision to be reconsidered, the University Data Protection Officer will reconsider the decision and respond within 21 days setting out the steps to be taken to comply with the individual's request.
- The University Data Protection Officer or other designated member of staff will document all correspondence in connection with this matter.