



## **CCTV System Policy**

### **1. Introduction**

- 1.1 The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at the University of Bradford, hereafter referred to as 'the University'.
- 1.2 The system comprises a number of fixed and fully functional (Pan/Tilt/Zoom) cameras located in buildings and externally around the University's three main Campus and associated satellite properties at Richmond Road (Main Campus), Emm Lane (School of Management) and Trinity Road (School of Health Studies). All cameras are monitored and recorded locally on the site where they operate, but are also monitored from a Central Control Room located on the main campus and are only available to security operational staff and security managers.
- 1.3 This Code follows Data Protection Act guidelines.
- 1.4 The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.
- 1.5 CCTV monitoring and recording systems will only be installed in or on University property when this has been reviewed and approved by the University Security Manager. Independently installed and operated CCTV systems by staff / students will not be permitted on any University property and where found actions will be taken to close these systems down. The only exception to this is the system that is registered and run by the Student Union in the Communal Building and Court Yard area on the main campus.
- 1.6 The CCTV system is owned by the University.

### **2. Objectives of the CCTV scheme**

- 2.1
  - (a) To protect University buildings and their assets
  - (b) To increase personal safety and reduce the fear of crime
  - (c) To support the Police in a bid to deter and detect crime
  - (d) To assist in identifying, apprehending and prosecuting offenders
  - (e) To protect members of the public and private property
  - (f) To assist in managing the Campus, its satellite properties and its car parks

### **3. Statement of intent**

- 3.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.
- 3.2 The University will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.
- 3.3 Cameras will be used to monitor activities within University buildings, on its campus areas, on its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of the University, together with its staff, students and visitors.
- 3.4.1 Security Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.
- 3.4.2 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained from Security Managers for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.
- 3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Video Tapes and / or Recorded Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Tapes and / or Recorded Data will never be released to the media for purposes of entertainment.
- 3.6 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
- 3.7 Warning signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by the University's CCTV and at the main entry / exit points of buildings in which CCTV cameras are installed. An example of the Warning Signs to be used can be found at appendix A.

### **4. Operation of the system**

- 4.1 The Scheme will be administered and managed by the University Security Manager, in accordance with the principles and objectives expressed in the code.
- 4.2 The day-to-day management will be the responsibility of both the Security Management Team (SMT) and the duty Security Supervisor during the day and the Duty Security Supervisor out of hours and at weekends.
- 4.3 The Control Room will only be staffed by SMT and the Duty Security Team .
- 4.4 The CCTV system will be operated 24 hours each day, every day of the year.

## **5. Control Room**

- 5.1 The Security Manager or his nominated deputy will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.
- 5.2 Access to the CCTV Control Room will be strictly limited to the SMT and the Duty Security Team. The door to the Control Room is to be kept secure at all times by on duty staff.
- 5.3 Unless an immediate response to events is required, staff in the CCTV Control Room must not direct cameras at an individual or a specific group of individuals.
- 5.4 Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangement as outlined below.
- 5.5 Control Room Operators must satisfy themselves over the identity of any other visitors to the Control Room and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be endorsed in the Control Room visitors log book.
- 5.6 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the Security Manager, or his nominated deputy and must be accompanied by him throughout the visit.
- 5.7 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- 5.8 If out of hours emergency maintenance arises, the Control Room Operators must be satisfied of the identity and purpose of contractors before allowing entry.
- 5.9 A visitors book will be maintained in the Control Room. Full details of visitors including time/date of entry and exit will be recorded.
- 5.10 There must always be at least one Control Room Operator present within the Control Room out of hours and weekends or the Control Room must be locked. During the working day when not manned the room must be kept secured.
- 5.11 Other administrative functions will include maintaining video tapes and hard disc space, filing and maintaining occurrence and system maintenance logs.
- 5.12 Emergency procedures will be used in appropriate cases to call the Emergency Services.

## **6. Liaison**

- 6.1 Liaison meetings may be held with all bodies involved in the support of the system.

## **7. Monitoring procedures**

- 7.1 Camera surveillance may be maintained at all times.

- 7.2 A viewing wall is installed in the main Control Room to which pictures will be continuously monitored, recording is carried out via Digital Data Recording or Video Tape machines as is required.
- 7.2 If covert surveillance is planned or has taken place copies of the written authorisation, including any Review, or Cancellation must be returned to the Director of Estates or his nominated deputy.

## **8. Digital recording procedures**

- 8.1 In order to maintain and preserve the integrity of the Digital Video Recorder (DVR) Hard Disks used to record events from the CCTV cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to:
  - 8.1.1 Each DVR must be identified by a unique mark or serial number
  - 8.1.2 Each DVR must be kept in a secure location with access restricted to authorised staff
  - 8.1.3 The controller shall check each DVR daily to ensure the system is operational
  - 8.1.4 A disk required for evidential purposes must be of the CD-R type only, disks will be provided in pairs each carrying an identical identification number, one a Master Disk to be retained by the University, the other a Copy which can be released to the police or other authorised third party on production of a signed data access request form. The disk should be loaded with the required CCTV data and viewer programme, identical information should be loaded on both Master and Copy disks. Each disk should be sealed in its own case using a tamper proof seal, the Master copy should be kept in a secure disk storage drawer. The Copy disk is handed to the person making the request on production of positive ID such as Police Warrant Card, Picture ID Card, Driver Licence, etc., the record sheet should then be completed and the Copy disk signed for and counter signed by the controller
  - 8.1.5 If data material is archived on the system, the reference number must be recorded on the record sheet
- 8.2 CCTV Recorded Images may be viewed by the Police for the prevention and detection of crime, authorised officers of the University of Bradford for supervisory purposes, authorised demonstration and training.
- 8.3 A record will be maintained of the release of Data on Disk to the Police or other authorised applicants. A register will be available for this purpose.
- 8.4 Viewing of CCTV Images by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

- 8.5 Should a Disk be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (iv) of this Code. Disks will only be released to the Police on the clear understanding that the Disk remains the property of the University, and both the disk and information contained on it are to be treated in accordance with this code. The University also retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained thereon. On occasions when a Court requires the release of an original disk this will be produced from the secure evidence disk draw, complete in its sealed case.
- 8.6 The Police may require the University to retain the stored disk(s) for possible use as evidence in the future. Such Disk(s) will be properly indexed and properly and securely stored until they are needed by the Police.
- 8.7 Applications received from outside bodies (e.g. solicitors) to view or release tapes will be referred to the Security Manager. In these circumstances tapes will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

## 9. **Video tape recording procedures**

- 9.1 In order to maintain and preserve the integrity of the tapes used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
- 9.1.1 Each tape must be identified by a unique mark.
- 9.1.2 Before using each tape must be cleaned of any previous recording.
- 9.1.3 The controller shall register the date and time of tape insert, including tape reference.
- 9.1.4 A tape required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence tape store. If a tape is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence tape store.
- 9.1.5 If the tape is archived the reference must be noted.
- 9.2 Tapes may be viewed by the Police for the prevention and detection of crime, authorised officers of the University of Bradford for supervisory purposes, authorised demonstration and training.
- 9.3 A record will be maintained of the release of tapes to the Police or other authorised applicants. A register will be available for this purpose.

- 9.4 Viewing of tapes by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.
- 9.5 Should a tape be required as evidence, a copy may be released to the Police under the procedures described in paragraph 9.1 (iv) of this Code. Tapes will only be released to the Police on the clear understanding that the tape remains the property of the University, and both the tape and information contained on it are to be treated in accordance with this code. The University also retains the right to refuse permission for the Police to pass to any other person the tape or any part of the information contained thereon. On occasions when a Court requires the release of an original tape this will be produced from the secure evidence tape store, complete in its sealed bag.
- 9.6 The Police may require the University to retain the stored tapes for possible use as evidence in the future. Such tapes will be properly indexed and properly and securely stored until they are needed by the Police.
- 9.7 Applications received from outside bodies (e.g. solicitors) to view or release tapes will be referred to the Security Manager. In these circumstances tapes will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

## **10. Breaches of the code (including breaches of security)**

- 10.1 Any breach of the Code of Practice by University security staff will be initially investigated by the Security Manager or his nominated deputy, in order for him/her to take the appropriate disciplinary action.
- 10.2 Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

## **11. Assessment of the scheme and code of practice**

- 11.1 Performance monitoring, including random operating checks, may be carried out by the Security Manager or his nominated deputy.

## **12. Complaints**

- 12.1 Any complaints about the University's CCTV system should be addressed to the Security Manager.
- 12.2 Complaints will be investigated in accordance with Section 10 of this Code.

## 13 Access by the Data Subject

- 13.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.
- 13.2 Requests for Data Subject Access should be made on an application form available from the Security Manager.
- 13.3 A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

The forms will also be available to the public, via the University Security Managers office in the Richmond Building.

## 14. Public information

Copies of this Code of Practice will be available to the public from the University Secretary's Office and the office of the Security Manager.

### Summary of Key Points

- This Code of Practice will be reviewed every two years.
- The CCTV system is owned and operated by the University of Bradford.
- The Control Room at the main campus will be manned 24 hours a day, 365 days a year.
- The Control Room is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies in Security Managers officers where CCTV Data can be viewed in private.
- Data recordings / tapes will be used properly, indexed, stored and destroyed after appropriate use.
- Data recording / tapes may only be viewed by Authorised University Officers, Security Control Room staff and the Police.
- Data Disks / tapes required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Data Disks / tapes will not be made available to the media for commercial or entertainment.
- Data Disks / tapes will be disposed of by a secure method.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the corporate policies and procedures of the University.
- Any breaches of this code will be investigated by the Security Manager. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the University Secretary.

**This document was produced April 2007 and is due to be reviewed April 2009**

**This CCTV System Policy document was reviewed by University Council and has been accepted. It will take effect from / /07.**

**Signed:** ..... **Position:** .....

**Print:** ..... **Date:** .....



**UNIVERSITY OF  
BRADFORD**  
MAKING KNOWLEDGE WORK



**CCTV**

**INFORMATION**

**24 HOUR CCTV SURVEILLANCE IN OPERATION.**

**Images are being monitored and recorded for the purposes of safety and the prevention and detection of crime. The organisation responsible for the system is the University of Bradford.**

**For further information contact the University Security Manager on 01274 234897.**