University of Birmingham

Closed Circuit Television (CCTV) Code of Practice

University of Birmingham uses closed circuit television (CCTV) images to provide a safe and secure environment for students, staff and visitors and to protect University property. This Code of Practice sets out the accepted use and management of CCTV equipment and images to ensure the University complies with the Data Protection Act 1998, Human Rights Act 1998 and other legislation. Where in this Code of Practice there is reference to the Data Protection Act or other legislation this includes all statutory amendments and subordinate legislation and regulations.

The University has produced this policy in line with the Information Commissioner's CCTV Code of Practice (www.ico.org.uk).

CCTV cameras are installed throughout the University's premises including car parks, residential accommodation, within buildings and externally in public areas. Many cameras are monitored and recorded within the security control room, which is a secure area. Those covering residential accommodation are monitored by Accommodation staff at Shackleton Hall. There are also individual building systems that are recorded locally but may not be monitored. This Code of Practice applies to all CCTV systems whether in use by any department in Corporate Services or within any of the Colleges and includes Webcams or other systems which capture images of identifiable individuals for the purpose of viewing and/or recording the activities of such individuals.

1. Purpose of CCTV

The University has installed CCTV systems to:

- Deter crime
- Assist in prevention and detection of crime
- Assist with the identification, apprehension and prosecution of offenders
- Assist with the identification of actions that might result in disciplinary proceedings against staff and students
- Monitor security of University buildings and areas
- Assist in traffic management and parking enforcement
- Promote a safe community environment

Before installing and using CCTV on University premises, the following steps must be taken:

- Assess and document the appropriateness of and reasons for using CCTV in that location
- Establish and document the purpose of the proposed CCTV system
- Establish and document who is responsible for compliance with this policy with regard to the proposed CCTV system
- Because CCTV involves the processing of personal data, register the CCTV system with the University's Information Compliance Manager, Legal Services
- From the date of issue of this Code of Practice all CCTV installations must be carried out by a University approved installer and not without prior consultation with the Head of Security.

2. Cameras

The University will make every effort to position cameras so that they only cover University premises as far as possible. No cameras will focus on private residential areas within University accommodation where avoidable, but will focus on public or shared areas. Camera operators who monitor cameras for the purpose of public space surveillance will receive SIA (Security Industry Authority) Licensing.

The situation of cameras should ensure that viewing does not intrude into neighbouring domestic areas that border the University's property as far as is practicable.

The University will clearly display signs in accordance with the Data Protection Act so that staff, students and visitors are aware they are entering an area covered by CCTV. Signs will state:

- The University is responsible for the CCTV system in that area
- The purpose(s) of the CCTV System
- Who to contact regarding the operation of the CCTV system

These signs can be produced internally by the relevant department with advice on wording from Legal Services or the Head of Security.

3. Images

Images produced by the equipment must be as clear as possible so that they are effective for the purpose(s) for which they are intended. The following standards must be adhered to:

- After installation, make a full check of the equipment to ensure it functions properly and works according to the operational requirement for which it was installed. No system shall be accepted until it is proven to work in all respects.
- Ensure that the recording media produces good quality images. Systems must record images digitally on the hard drive of a Digital Video Recorder and be capable of being transferred to removable media such as CD, both in the form of still and moving images.
- Recording media must not continue to be used if it becomes clear that the quality of the images is not of a sufficient standard.
- Time/date recordings must be continually verified as accurate as they are crucial from an evidential point of view.
- Cameras must be located so they will capture images relevant to the purpose(s) for which the system has been installed and of suitable quality.
- Cameras must be properly maintained and serviced and maintenance logs kept. All CCTV systems must be subject to a minimum of annual maintenance checks.
- The operator of the system must carry out regular audits on the system checking each camera systematically to ensure full function and also take a specimen recording to ensure the recording function is working. All such audits must be documented and kept.
- In the event that cameras become unserviceable, there must be clear intention for getting them repaired and working within a specific time period, normally within 48 hours.
- Cameras that may be at risk of vandalism due to their location must be protected so that they are kept in working order.

- Monitors displaying CCTV images of non public areas must be located so that they can only be viewed by staff authorised to use the equipment.

4. Retention

CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and in any event will not be held for more than 31 days except where they need to be retained longer for evidential purposes. In such cases the images will be stored on removable media and will be held securely by the system owner until such time as handed over to the police or other authorised body (see Section 6). Images stored on removable media such as CDs will be erased or destroyed once the purpose of the recording is no longer relevant.

5. Covert Recording

The University may only undertake covert recording with the written authorisation of the Registrar and Secretary (or in his absence the Director of HAS or the Director of Legal Services) at the request of the request of the Head of Security or in his absence the Security Operations Manager.

Covert recording can only be undertaken where:

- Informing the individual(s) concerned that recording is taking place would seriously prejudice the reason for making the recording; and

- There is good cause to suspect that an illegal or unauthorised action(s) is/are taking place or about to take place and the use of CCTV systems to detect such activity is justified

Any such monitoring will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring and only for a specific illegal or unauthorised activity. All such occasions will be fully documented showing when and why the decision to use covert monitoring was made.

6. Disclosure of Images to Third Parties (Excluding Data Subjects)

Disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected, and also that the images can be used as evidence if required. Images can only be disclosed in accordance with the purposes for which they were originally collected and in accordance with the Data Protection Act.

Access to recorded images will be restricted to those staff or external agencies authorised to view them and will not be made more widely available. Viewing of recorded images must take place in a restricted area to which other employees, students or members of the public will not have access while viewing is occurring. If media on which images are recorded are removed for viewing purposes, this must be documented. Images retained for evidence must be securely stored.

The following information must be recorded when media are removed for viewing by authorised persons:

- Date and time they were removed

- The name of the person removing the media

- The name(s) of the person(s) viewing the images

- The name of the University department to which the person viewing the images belongs, or the person's organisation if they are from outside the University

- The reason for viewing the images
- The date and time the media were returned to the CCTV system or secure storage

Disclosures to third parties will only be made in accordance with the purpose(s) for which the CCTV system is used and will be limited to:

- Police and other law enforcement agencies
- Relevant legal representatives as defined by the Civil Procedure Rules
- Data subjects whose images have been recorded and retained in accordance with section 7 below (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
- Members of staff authorised to review and retain copies of recorded images as part of the management of internal procedures within the University such as disciplinary procedures
- Where the disclosure is authorised by law or in compliance with a court order

All requests for disclosure must be documented. If disclosure is denied, the reason must also be recorded. In addition to the information required above, the following must also be documented:

- If the images are being removed from the CCTV system or secure storage to another area, the location to which they are being transferred
- Any crime incident number, if applicable
- The signature of the person to whom the images have been transferred on a formal written receipt as acknowledgement of transfer

7. Individual Access Rights by Data Subjects

The Data Protection Act gives individuals (data subjects) the right to access personal information about themselves, including CCTV images. All requests for access to images by data subjects (when they are asking for access to images of themselves) should be made in writing to the University's Legal Services for the attention of the Information Compliance Manager. The manager responsible for the system will liaise with the Information Compliance Manager to determine whether disclosure of the images will reveal third-party information. Requests for access to CCTV images must include sufficient information to enable the University to identify:

- The date and time when the images were recorded
- The location of the CCTV camera
- Further information to identify the individual, if necessary

The payment of a fee for disclosure will be in accordance with the University's Data Protection Policy. The University is required by the Data Protection Act to respond promptly and at the latest within 40 days of receiving the fee and sufficient information to identify the images requested. If the University cannot comply with the request, the reasons must be documented. The requester will be advised of these in writing, where possible. Decisions regarding the disclosure of information following a request from a data subject will be made and communicated to the requester by Legal Services in accordance with the University's Data Protection Policy.

8. Responsibility for CCTV systems

For CCTV systems operated anywhere within the University, the ultimate responsibility for compliance with this Code of Practice lies with the Registrar and Secretary.

The Head of Security is tasked with the responsibility for CCTV systems within non-residential areas that fall within the responsibility of the Directorate of Hospitality and Accommodation Services (HAS) and which are connected for viewing purposes to the Security Control Room.

Systems installed within residential accommodation are the responsibility of the General Manager, Student Accommodation, HAS

Systems installed by other University departments are the responsibility of the relevant Head of College or Corporate Service area.

9. Staff Training

University departments that have installed CCTV systems must ensure that persons handling CCTV images or recordings have received training in the operation and administration of the system before use. Concerns regarding the application of the Data Protection Act or other legislation should be referred to Legal Services.

10. Complaints

Complaints and enquiries about the operation of the University's CCTV systems should be made in writing in the first instance to those having day-to-day responsibility as specified in section 8. If a complainant is not satisfied with the response received, they should write to the Director of Hospitality and Accommodation Services (HAS). Complainants can also make a complaint directly to the Information Commissioner's Office at www.ico.org.uk or by calling 0303 123 1113.

11. Monitoring Compliance

Under the Registrar and Secretary, Legal Services are responsible for providing advice with regard to the compliance of CCTV systems with the Data Protection Act and other legislation. The Head of Security can provide expert guidance with regard to the installation, management and operation of such systems. Systems which are deemed to be non compliant with this Code of Practice must be made compliant within a specified period of time or must be decommissioned. Responsibility for ensuring that a CCTV system is compliant rests with the Head of College or Corporate Service area or the person to whom they have delegated such responsibility.

Enquiries relating to the Data Protection Act 1998 or other relevant legislation should be referred to the Information Compliance Manager within Legal Services. The University's Data Protection Policy can be found at:

www.birmingham.ac.uk/documents/university/legal/data-prot-policy.pdf