Closed Circuit Television (CCTV) Policy

1 Introduction

Brunel University London uses closed circuit television (CCTV) images to provide a safe and secure environment for students, staff and visitors, and to protect University property.

This document sets out the accepted use and management of the CCTV equipment and images to ensure the University complies with the Data Protection Act 1998, Human Rights Act 1998 and other legislation.

The University has produced this policy in line with the Information Commissioner's CCTV Code of Practice.[1]

2 Purpose of CCTV

Policy

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 campus buildings
- identify vehicle movement problems around the campuses.

1 http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf

Guidance

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

1. Assess and document the appropriateness of, and reasons for, using CCTV.

2. Establish and document the purpose of the proposed scheme.

3. Establish and document who is responsible for day-to-day compliance with this policy.

4. Because CCTV involves the processing of personal data, register the scheme with the Information Access Officer before using the system, so s/he can ensure it is covered by the University's Notification with the Office of the Information Commissioner.

3 Covert recording

Policy

The University may only undertake covert recording with the written authorisation of the Chief Operating Officer where:

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

- there is good cause to suspect that an illegal or unauthorised action(s) is/are taking place or about to take place.

Guidance

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 unauthorised activity.

All such occasions will be fully documented showing who made the decision to use covert monitoring and why.

4 Cameras

Policy

The University will make every effort to position cameras so that they only cover University premises.

No cameras will focus on University residential accommodation, public areas and entrances excepted. Camera operators will receive training and written procedures for maintaining the privacy of the occupants of such accommodation.

The University will clearly display signs so that staff, students and visitors are aware they are entering an area covered by CCTV.

Guidance

If, for any reason, any neighbouring domestic areas that border the University's property are included in the camera view, the occupants of the property will be consulted prior to any recording, or recording for those areas will be disabled.

Signs will state:

- Brunel University London is responsible for the CCTV scheme
- the purpose(s) of the scheme
- whom to contact regarding the scheme.

5 Images

5.1 Quality

Policy

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.

Guidance

The following standards must be adhered to:

1. After installation, make an initial check of the equipment to ensure it works properly.
2. Ensure that tapes, where used, are of good quality.
3. Do not continue to use media once it becomes clear that the quality of the images has begun to deteriorate.
4. Where the location of the camera and time/date are recorded, these should be accurate. Document the system for ensuring accuracy.
5. Site the cameras so they will capture images relevant to the purpose(s) for which the scheme has been established.
6. Assess whether it is necessary to carry out constant real-time recording, or only at certain times when suspect activity usually occurs or is likely to occur.

7. Cameras should be properly maintained and serviced and maintenance logs kept.

8. Protect cameras from vandalism so that they are kept in working order.

9. In the event that cameras break down or are damaged, there should be clear responsibility for getting them repaired and working within a specific time period.

5.2 Retention

Policy

Images and recording logs will be held in accordance with the University's Records Retention and Disposal Policy and associated schedules.

Guidance

Refer to the Records Retention and Disposal Policy and the Records Retention and Disposal Schedules for information on analogue recording systems and recording logbooks.

For digital recording systems, 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. Images stored on removable media such as CDs will be erased or destroyed once the purpose of the recording is no longer relevant. All digital recordings will be digitally watermarked to maintain integrity.

Recording media no longer in use will be securely destroyed.

6 Access to and disclosure of images to third parties

Access to, and disclosure of, images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are retained, and also ensure 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 University's Notification to the Office of the Information Commissioner.

This document separates access and disclosure into two subsections.

6.1 Access to images

Policy

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

Monitors displaying images from areas in which individuals would have an expectation of privacy should only be seen by staff authorised to use the equipment.

Viewing of recorded images should take place in a restricted area to which other employees will not have access while viewing is occurring.

If media on which images are recorded are removed for viewing purposes, this should be documented.

Images retained for evidence should be securely stored.

Guidance

Document the following information when media are removed for viewing:

1. Date and time they were removed
2. The name of the person removing the media
3. The name(s) of the person(s) viewing the images.
4. 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.
5. The reason for viewing the images
6. The date and time the media were returned to the system or secure storage.

6.2 Disclosure of images

Policy

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

- police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder*
- prosecution agencies
- relevant legal representatives
- advisors from the Advice and Representation Centre of the Union of Brunel Students
- people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)
- in exceptional cases, to others to assist in identification of a victim, witness or perpetrator in relation to a criminal incident
- members of staff involved with University disciplinary processes.

***The Chief Operating Officer, or his/her designated agent, is the only person who can authorise disclosure of information to the police or other law enforcement agencies.**

All requests for disclosure should be documented. If disclosure is denied, the reason should also be recorded.

Guidance

In addition to the information required in section 6.1 above, the following should be documented:

1. If the images are being removed from the CCTV system or secure storage to another area, the location to which they are being transferred.
2. Any crime incident number, if applicable.
3. The signature of the person to whom the images have been transferred.

7 Individuals' access rights

Policy

The Data Protection Act 1998 gives individuals the right to access personal information about themselves, including CCTV images.

All requests for access to images by individuals (when they are asking for access to images of themselves) should be made in writing to the University's Information Access Officer. A form available to use at http://www.brunel.ac.uk/about/administration/information-access/data-protection/policies-and-guidelines, but an e-mail with sufficient information to locate the images is acceptable.

The manager responsible for the system will liaise with the Information Access Officer to determine whether disclosure of the images will reveal third-party information.

Guidance

Requests for access to CCTV images must include:

- the date and time when the images were recorded
- the location of the CCTV camera
- further information to identify the individual, if necessary
- payment of a fee of £10.

The University will respond promptly and at the latest within 40 days of receiving the fee and sufficient information to identify the images requested.

Staff responsible for CCTV systems will refer all such requests to the Information Access Officer.

If the University cannot comply with the request, the reasons must be documented. The requester will be advised of these in writing, where possible.

If there is any doubt about what information must be provided to enquirers, please contact the Information Access Officer.

8 Responsibility for CCTV systems

For systems operated by Operations, the overall responsibility lies with the Chief Operating Officer.

The Security Manager is tasked with day-to-day responsibility within Operations.

For systems operated by Accommodation & Residences, the overall responsibility lies with the Director, Accommodation & Residences.

Day-to-day responsibility is as follows:

- Accommodation: relevant Residences Manager
- Catering/Bars: Head of Catering Services.

9 Staff Training

The Chief Operating Officer and Director, Accommodation & Residences will ensure that staff handling CCTV images or recordings receive training on the operation and administration of the CCTV systems. In addition, they will liaise with the Information Access Officer to ensure training is provided on the impact of the Data Protection Act 1998 with regard to those systems.

10 Complaints

Complaints and enquiries about the operation of the University's CCTV systems should be addressed to those having day-to-day responsibility, as listed in section 8 above.

Enquiries relating to the Data Protection Act should be addressed to the Information Access Officer, Governance, Information & Legal Office (e-mail: data-protection@brunel.ac.uk).

If a complainant or enquirer is not satisfied with the response received, they should write to the Secretary to Council.

11 Monitoring Compliance

Heads of relevant areas will undertake occasional reviews with the Information Access Officer to ensure updating of knowledge and compliance with this policy and relevant legislation.

Change notice

Modifications made 08 February 2012:

- Added bullet point regarding the Advice and Representation Centre in section 6.2
- Changed all references to 'Director, Resources and Operations' to read 'Chief Operating Officer'
- Changed logo on first page
- Changed URL for subject access form in section 7

Modifications made 11 November 2014:

- Changed logo and font
- Changed unit names for operators of CCTV systems
- Changed unit name for Information Access Officer

Modifications made 20 May 2015

- Changed University name to Brunel University London