UNIVERSITY COLLEGE LONDON

CCTV POLICY

Endorsed by the Security Working Group - 17 October 2012

Endorsed by the Infrastructure IT Services Strategy Group - 18 October 2012

Reviewed and endorsed (with one change) by HR

Approved by the Director of Estates – 4 September 2013

1. Purpose and objectives

This policy forms part of University College London's commitment to the safeguarding of personal data. Its objective is to help staff and students understand their rights and obligations with respect to the use of closed circuit television (CCTV) systems in UCL.

2. Introduction

UCL processes the personal data of living individuals such as its staff, students, contractors, research subjects and customers, including images captured by CCTV systems. This processing is regulated by the Data Protection Act 1998 (DPA) and the Information Commissioner's *CCTV code of practice*. The UK's regulator for the DPA is the Information Commissioner's Office.

It is the duty of data controllers such as UCL to comply with the data protection principles with respect to personal data. This policy describes how UCL will discharge its duties in order to ensure the continuing compliance of its CCTV systems with the DPA in general and the data protection principles and the *CCTV code* in particular.

3. Scope

This policy is a supporting policy of the UCL Information Security Policy. Its scope is as defined in section 1.4 of that Policy:

> "The policy applies to all staff and students of UCL and all other computer, network or information users authorized by the College or any department thereof. It relates to their use of any UCL-owned facilities (and those leased by or rented or on loan to UCL), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to the UCL network; to all UCL-owned or licensed data and programs (wherever stored); and to all data and programs provided to UCL by sponsors or external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of UCL business."

4. Definitions

Personal Data[1]

> '"Personal data" means data which relate to a living individual who can be identified—

[1] DPA section 1

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'

Processing[2]
Obtaining, recording or holding personal data. This includes organisation, adaptation or alteration; retrieval, consultation or use; disclosure; and alignment, combination, blocking, erasure or destruction.

Data Controller
As the organisation which determines the purposes of the processing, UCL is the Data Controller for the personal data that it manages.

Data Protection Officer
The UCL member of staff with lead responsibility for UCL's compliance with the DPA.

Data Subject[3]
A living individual who is the subject of personal data

Data Processor[4]
Any third party (other than UCL staff and students) who processes personal data on behalf of and on the instructions of the Data Controller.

5. Roles and responsibilities

Head of Facilities Services
The Head of Security & Facilities Services is responsible for the approval and running of CCTV systems on all UCL premises.

Security Manager
To provide, procure and review a fully staffed security service to the entire UCL Campus and provide protection of the staff, students, visitors, assets and other property through the provision of a safe and secure working environment.

To manage the day to day running of the Security Control room and the Control room Manager and to ensure all policies and procedures are kept up to date and implemented.

The provision of the service includes developing and reviewing the strategy for the procurement and operation of staffed services, financial and physical resource planning and control and, full day to day operation of all physical security activities on a 24/7/365 basis.

Control Room Manager
The Control Room Manager is responsible for the assessment and definition of operational requirements before the installation of any CCTV cameras takes place. This should include a statement of the problem, a risk assessment and determination

[2] DPA section 1
[3] DPA section 1

of success criteria, as well as the identification of system requirements and a consideration of operational issues. Management issues should be considered in consultation with relevant colleagues.

After installation, the Control Room Manager is also responsible for validation of the cameras, ensuring successful testing of field of view, quality of live and recorded images, storage capabilities of the system and the operation of all alarms and motion detection features.

Duty Controllers
Are responsible for the daily operation of the system which includes but is not limited to reviewing footage and providing evidence, ensuring access to the control room is controlled and all access is documented in the relevant logs. Reporting all faults to the control room manager, ensuring all views are correct and relate to the specific purpose of the camera, performing daily checks to ensure the system is working as per its intended use. To monitor live images throughout the site for the purpose of security, health and safety and management of the Security staff.

Data Protection Officer
The Data Protection Officer (DPO) (data-protection@ucl.ac.uk) has primary responsibility for UCL's compliance with the DPA. This comprises:

- maintaining UCL's notification with the Information Commissioner's Office
- ensuring completion of the Annual Survey of Personal Data Holdings
- handling subject access requests and requests from third parties for personal data
- promoting and maintaining awareness of the DPA and regulations, including training
- investigating losses and unauthorised disclosures of personal data.

The DPO is UCL's main contact for the Information Commissioner's Office.

Heads of Department / Division
Heads of Department / Division are responsible for ensuring their staff understand the role of the data protection principles in their day-to-day work, through induction, training and performance monitoring, and for monitoring compliance within their own areas of responsibility. They should also ensure Data Protection Coordinators are designated for their departments or divisions, and provided with appropriate training and support.

Data Protection Coordinators
Coordinators are required to:

- advise staff and students in their departments on the implementation of and compliance with this policy and any associated guidance / codes of practice
- ensure appropriate technical and organisational measures are taken within their departments to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- support UCL's notification with the Information Commissioner's Office by maintaining the register of holdings of personal data, including CCTV, and the purposes of processing

- keep the Data Protection Officer informed of changes in the collection, use, and security of personal data within their department
- report any loss of personal data to the Head of Department / Division and the Data Protection Officer.

Data Processors
Data processors have a contractual responsibility to act only on UCL's instructions and to ensure that their processing of personal data provided by UCL is carried out in compliance with this policy and in accordance with the eight data protection principles. There should be a written agreement with data processors which adequately addresses these responsibilities.

Staff and students
All staff and students are responsible for:

- raising any concerns in respect of the processing of personal data with the Data Protection Officer
- promptly passing on to the Data Protection Officer all subject access requests and requests from third parties for personal data
- reporting losses or unauthorised disclosures of personal data to the Data Protection Coordinator.

6. Purposes of processing

UCL seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors and contractors, whilst within or situated on its premises. CCTV cameras and recording devices are deployed in order to:

- assist in the reduction, prevention and detection of crime
- assist with the identification, apprehension and prosecution of offenders
- monitor the security of buildings
- identify vehicle movement problems around the estate
- assist with safety and security management
- provide evidence which may be used by the police or others to prosecute offenders
- enhance public safety
- support protection of property.

The Information Commissioner's CCTV Code of Practice[4] also allows for employers to use images in circumstances which they cannot be reasonably expected to ignore, including criminal activity, gross misconduct or where behaviour is likely to put others at risk. (Gross misconduct is defined in the UCL Disciplinary Policy and Procedure.[5])[

7. Use of images

Personal data (i.e. images of individuals obtained by UCL's CCTV systems) may only be used in connection with the stated purposes.

Surveillance must be proportionate to the problem. Cameras provide fields of view encompassing approaches to building entrances, building property lines and internal

[4] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf
[5] http://www.ucl.ac.uk/hr/docs/disciplinary_procedure.php

communal and secure areas. They will be situated so that they only capture images relevant to the purpose for which the system has been established, and to ensure they do not capture areas not intended to be the subject of surveillance. Where appropriate, recording will take place only at times when a problem usually occurs.

With the exception of wide angle or long distance shots, third party domestic or commercial premises are not included in any camera's field of view. Where applicable Pan Tilt & Zoom cameras will be programmed with a normally parked position and third party views will be masked within the camera's field of view.

Sound recording is not permitted. Where a system is used which permits sound recording, this function must be disabled. Wireless cameras are not used.

Images of staff and students used in disciplinary proceedings will be made available to the subjects of investigations or their representatives to provide them with an opportunity to respond.

7.1 Covert Monitoring

Covert monitoring may be used as part of a specific time-limited investigation where informing data subjects that monitoring is taking place would prejudice that investigation. The decision to use covert monitoring may only be taken with written authorisation from one of the following (or authorised delegate) as appropriate: the Director of Human Resources (where monitoring relates to matters in respect of staff); the Registrar (where monitoring relates to matters in respect of students); the Director of Estates and Facilities (where monitoring relates to matters in respect of premises).

In addition to the above authority, written authorisation must be obtained from the Head of Facilities Services and the UCL Data Protection Officer.

Covert monitoring shall only be used for the prevention and detection of criminal activity or equivalent malpractice.

7.2 Expectation of Heightened Privacy

In places where there is a reasonable expectation of heightened privacy, such as lavatories or changing rooms, surveillance (as distinct from covert monitoring) will only take place in the most exceptional circumstances where there is a suspicion of serious crime; there must also be an intention to involve the police. This will be decided by the Head of Facilities Services, in consultation with the Data Protection Officer and in accordance with part 8 of this policy.

7.3 Continuous Monitoring of Staff and Contractors

Continuous monitoring of staff and contractors will be used in exceptional circumstances, where failure to follow instructions would endanger personal safety. The decision to use continuous monitoring will only be taken by the Director of Human Resources in consultation with the Data Protection Officer.

8. Signage

Signs must be placed so that people are aware they are entering an area which is covered by CCTV cameras. Signs must:

- be clearly visible and legible
- be of a size appropriate to the circumstances

Signs must contain the following information:

- the name of the Data Controller (i.e. UCL)
- the purpose(s) of the scheme
- a contact telephone number for enquiries.

Signs must contain the following wording:

"Images are being recorded for the purposes of detection and prevention of crime and safety and security management."

There is no requirement for signage in instances of covert monitoring as defined in paragraph 7 (1) above.

9. Operating standards

9.1 Control Rooms

Details of the administrative procedures which apply to all Security Control Rooms must be set out in the procedure manual, which should include technical instructions on the use of the equipment and a schedule of maintenance.

Control Rooms will be staffed in accordance with the procedure manual. Equipment associated with the system will only be operated by authorised staff. The Control Room Manager will ensure that all staff are fully briefed and trained in respect of the functions, operational, administrative and legal, arising from the use of CCTV.

All staff working in a Control Room will be made aware of the sensitivity of handling CCTV images and recordings. A copy of this Policy and the procedure manual will be held in the Security Control Room at all times for staff to consult. They must be familiar with the contents of both documents, which will be updated from time to time, and must comply with both as far as is reasonably practicable at all times.

Images are monitored and recorded centrally in the Security Control Room or locally on the site where they operate. The equipment has the capability to record on all cameras simultaneously throughout every 24 hour period.

Operators may be required to justify their interest in or recording of, any particular individual, groups of individuals or property at any time by the Control Room Manager or Head of Security & Facilities Services

Recorded images may only be viewed by authorised persons at designated locations. The Control Room Manager is responsible for the evaluation and approval of suitable locations and must maintain a record of all locations and authorised persons.

9.2 Access to Control Rooms

Viewing areas must be secure against unauthorised access. Monitors showing recorded images must be positioned so that images cannot be viewed by an unauthorised person. Access is limited to Duty Controllers, authorised members of

senior management, police officers and any other person with statutory powers of entry.

Staff, students or visitors may be granted access to a Control Room on a case-by-case basis by the Head of Security & Facilities Services, Security Control Room Manager or Senior Operations Manager who must sign the authorisation within the relevant visitors' log book. Access will only be provided in order to help with the identification of individuals.

Before allowing access to a Control Room, staff will satisfy themselves as to the identity of any visitor and that the visitor has appropriate authorisation from the Control Room Manager or Security Manager. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation, the person who granted authorisation and the times of entry to and exit from the Room. A similar log will be kept of the staff on duty in a Control Room.

Arrangements may be made for police or other third parties to be present in the Security Control Room at certain times. Under extreme circumstances the Police may make a request to assume direction of the system to which this Policy applies. Only requests made on the written authority of a police officer not below the rank of Superintendent will be considered. Any such request will only be accommodated on the personal written authority of the Head of Security & Facilities Services, or designated deputy of equal standing. In the event of a request being granted, the Control Room will continue to be staffed, and equipment operated by, only those personnel who are authorised to do so.

9.3 Quality of recorded images

Images produced by the recording equipment must be as clear as possible in order that they are effective for the purpose for which they are intended. Recorded pictures and prints as well as live screens should produce clear pictures. The effects of compression on image quality must be checked.

To maintain the evidential integrity of images and support effective retrieval, metadata to be recorded with the images should include the date, time, and camera location and number. These must be regularly checked and maintained.

The activity of taking copies should not interfere with the operation of the system.

9.4 Maintenance

Cameras must be properly maintained and serviced to ensure that clear images are recorded a log of all maintenance activities will be kept. A daily check should be made of camera functions (including PTZ function), alignment, and image quality. In addition, an annual check should be made of camera housings and cabling in accordance with the maintenance schedule as specified by the Control Room Manager.

9.5 Production of copies

When single images and short video clips are to be exported from the main CCTV recording system, they must be copied to "write-once" media (e.g. finalised CDROM or DVDROM) which carries an indelible serial number, so that a complete audit trail is maintained. A secure register of copies made must be kept. Any temporary copies made during the export process must be destroyed as soon as it is clear that the export has been successful.

Personnel carrying out copying must be authorised and trained. Training must include awareness of how systems can make unobvious temporary copies, such as in browser caches.

9.6 Retention periods

CCTV images must not be retained for more than 18 days. There are two exceptions to this rule:

1. Where images have been approved for disclosure to a third party, they may be held until they can be collected.
2. When necessary in order to establish patterns of behaviour over a longer period, images will be retained pending any action being taken. To ensure compatibility with the 5th data protection principle, such cases must be documented. A written case must be made by the Security Manager or Control Room Manager and reviewed frequently.

Exported images must be stored securely when not in use. The media must be destroyed when the images are no longer required, with a log kept of that destruction.

10. Access to images

Data subjects have a right of access to their personal data, including CCTV images of themselves.

Subject access requests must be made in writing, including Form 6 (http://www.ucl.ac.uk/efd/recordsoffice/data-protection/) or otherwise and sent to the Data Protection Officer. Data subjects must prove their identity.

Copy images, if held, will be provided promptly and in any event within 40 days.

UCL does not charge a fee for subject access requests.

Where disclosure of images would lead to an unfair intrusion into the privacy of third parties, or unwarranted harm or distress, images of those third parties will be redacted.

In certain circumstances the DPA provides for disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the police, UK Border Agency, local authorities or sponsors, should be made in writing and handled by the Data Protection Officer.