

# CCTV POLICY STATEMENT

## 1.0 Owner

- 11 London Metropolitan University has in place and is further developing a CCTV surveillance system, “the system” on the College site. Images are monitored and recorded centrally and will be used in accordance with this Policy and its notified purposes. London Metropolitan University owns the system.
- 12 The Data Controller is responsible for the operation of the system and for ensuring compliance with this Policy. They may be contacted as follows:

Data Controller                      London Metropolitan University  
Tower Building  
166-220 Holloway Road  
London  
N7 8DB

Contact                                      Peter Fisher  
Records and Compliance Officer  
Room JS2-80a  
Jewry Street  
[Email: p.fisher@londonmet.ac.uk](mailto:p.fisher@londonmet.ac.uk)

## Data Protection Act 1998

CCTV images that show a recognisable person, are Personal Data and are covered by the Data Protection Act. This Policy is associated with the London Metropolitan University Data Protection Policy, the provisions of which should be adhered to at all times.

The Data Protection Officer, who is responsible for the London Metropolitan University Data Protection Policy is:

Mr Peter Fisher  
London Metropolitan University  
Room 80A  
2<sup>nd</sup> Floor  
31 Jewry Street  
London  
EC3N 2EY

[Email: p.fisher@londonmet.ac.uk](mailto:p.fisher@londonmet.ac.uk)

## **20 The System**

- 21 *The system comprises: Fixed position cameras; Pan, tilt and zoom cameras; Dome cameras; Monitors: Multiplexers; Video recorders designated record only; Video recorders designated playback only; Digital recorders; Magnetic tape erasers; Public information signs; Recording media.*
- 22 *Cameras will be located at strategic points on the campus, principally at the entrance and exit points of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation or, alternatively, operatives will be instructed and trained on the importance of the individual's right to expect privacy.*
- 2.3 *Signs will be prominently placed at strategic points of the campus to inform staff, students, visitors and members of the public that a CCTV installation is in use, its purpose and contact details for further information, if required.*
- 24 Although every effort has been made to ensure the effectiveness of the system, it is not possible to guarantee that the system will detect every or any incident which takes place within the intended area of coverage.

## **3.0 Purpose of the System**

- 31 The system has been installed by London Metropolitan University with the primary purpose of reducing the threat of crime generally, protecting London Metropolitan University's premises and helping to ensure the good health and safety of all London Metropolitan University's staff, students and visitors, together with good general and property management consistent with respect for the individual's privacy.

The system will not be used:

- to provide recorded images for the world-wide-web.
- to record sound other than in accordance with the legal requirements of the Data Protection Act on covert recording.
- for any automated decision-making relating to staff.

### **31 Covert Recording**

3.2.1 Covert cameras may be used under the following circumstances on the written authorisation or request of the Director of Estates and Facilities and where it has been assessed by at least two of the senior staff listed at Appendix 2:

- that informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and where the Data Controller has:
  - a) Identified specific criminal activity.
  - b) Identified the need to use surveillance to obtain evidence of that criminal activity.
  - c) Assessed whether the use of signs would prejudice success in obtaining such evidence.
  - d) Assessed how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary.
  - e) Documented (a) to (d) above.

3.2.2 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected criminal activity.

3.2.3 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

#### **4.0 The Control Room**

- 4.1 Images captured by the system may be monitored and recorded in the Control Room, twenty-four hours a day throughout the whole year. Images displayed on monitors will not be visible from outside the Control Room and/or monitors will be screened.
- 42 No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the Duty Controllers, authorised members of senior management, authorised service or maintenance personnel, to satisfy a Subject Access Request, Police Officers and any other person with statutory powers of entry.
- 43 Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the Visitor's Log, which shall include details of their name, their department or organisation they represent (where appropriate), the person who granted authorisation and the times of entry to and exit from the Control Room. A similar log will be kept of the staff on duty in the Control Room and any visitors granted emergency access.

## **50 Control Room Administration and Procedures**

- 51 Details of the administrative procedures, which apply to the Control Room, will be set out in a Procedures Manual, a copy of which may be requested by prior arrangement, stating the reasons for the request.
- 5.2 It is recognised that images may be sensitive material and are subject to the provisions of the Data Protection Act 1998; the Facilities Manager is responsible for ensuring day to day compliance with the Act. All recorded material will be handled in strict accordance with this Policy, the Data Protection Act and the procedures set out in the University CCTV Code of Practice.

## **6.0 Staff**

- 61 All staff working in the Control Room will be made aware of the sensitivity of handling CCTV images and recordings. The Facilities Manager will ensure that all staff are fully briefed and trained in respect of the functions, both operational and administrative, arising from the use of CCTV.

## **70 Recording**

- 71 Where digital recording equipment is employed, digital recordings will be backed up onto VCR. Analogue recordings are made using video tape recorders operating in time lapse mode. Incidents may be recorded in real time.
- 72 Each tape will be uniquely identified and all activities associated with it will be recorded in the Tape Log up to and including its final erasure and disposal. The Tape Log will be kept secure and access to it will only be provided to the relevant member of staff.
- 73 Recorded images will normally be retained for twenty-eight days from the date of recording, erased and reused on no more than thirteen consecutive occasions. Once a tape has reached the end of its use it will be erased prior to disposal and the Tape Log will be updated accordingly.
- 74 All recordings and images shall remain the property of London Metropolitan University until disposal and destruction.

## **80 Access to Recording and Copies**

- 81 All access to recorded images will be recorded in the CCTV Code of Practice Access Log.
- 82 Access to recordings will be restricted to those staff who need to have access in accordance with the purposes of the system.

83 Access to tapes by third parties

8.3.1 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings
- Emergency services in connection with the investigation of an accident

84 Access to recordings by a subject

CCTV film, if it shows a recognisable person, is Personal Data and is controlled by the Data Protection Act. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the recording, subject to the prohibitions on access also covered by the Data Protection Act. They do not have the right of instant access and must abide by the Data Protection Procedures.

8.4.1 A person whose image has been recorded and retained and who wishes access to the recording must apply in writing to the Data Protection Officer. The request must be made using a standard Subject Access Request form which can be downloaded from:

<http://www.londonmet.ac.uk/data-protection>

The £10.00 fee must accompany this request.

8.4.2 The Data Protection Officer will then consider the request and, where granted, will arrange for a copy of the recording to be made available to the applicant. The applicant must not ask another member of staff to show them the recording or ask anyone else for a copy of the film. All communications must go through the London Metropolitan University Data Protection Officer. A response will be provided promptly and, in any event, within forty days of receiving the required fee and information.

8.4.3 The Data Protection Act gives the Data Controller the right to refuse a request for subject access, particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

8.4.4 If it is decided that a Data Subject Access Request is not to be complied with, the reasons will be fully documented and the data subject informed, whenever possible in writing, stating the reasons.

## **90 Request to Prevent Processing**

- 91 All such requests should be addressed in the first instance to the Data Protection Officer, who will provide a written response within twenty-one days of receiving the request, setting out their decision on the request. A copy of the request and response will be retained.

## **10 Complaints**

- 10.1 It is recognised that members of London Metropolitan University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instance to the Facilities Manager. The complaints procedure can be found on the University's website: <http://www.londonmet.ac.uk/student-services/policies-and-procedures/complaints-procedure.cfm>

## **11 Compliance Monitoring**

- 11.1 The contact point for members of London Metropolitan University or members of the public wishing to enquire about the system will be via the Facilities Manager which will be available during the hours of 0900 and 1200 and 1400 and 1700 Monday to Friday except when London Metropolitan University is officially closed.
- 11.2 Upon request enquirers will be provided with:
- A summary of this statement of policy
  - An access request form if required or requested
  - A subject access request form if required or requested
  - A copy of the London Metropolitan University central complaints procedures
- 11.3 All documented procedures will be kept under review and a report periodically made to the Data Controller.

## **Appendix 1**

### **Authorised Access to the Communications Centre**

---

Other than Communications Centre personnel, the following have authorised access to the Communications Centre:

Facilities Manager  
Deputy Facilities Managers

**Appendix 2**

Those authorised access to recordings in order to achieve the purposes of the system:

Those persons included under paragraph 4.2 including Duty Controllers, authorised members of senior management, authorised service or maintenance personnel to satisfy a Subject Access Request, Police Officers and any other person with statutory powers of entry.

Director of Human Resources

Deputy Vice Chancellor – Academic

Deputy Vice Chancellor – Research and Development

Director of Finance

University Secretary

**SUBJECT ACCESS REQUEST FORM**

**Are you a member or former member of staff?**

Yes/No

**1 Details of the person requesting the information**

Full Name .....

Address .....

.....

Telephone Number ..... Fax Number .....

Email .....

**2 Are you the Data Subject?**

**YES** If you are the Data Subject, please supply evidence of your identity, i.e. library card, driving licence, birth certificate (or photocopy) and, if necessary, a stamped addressed envelope for returning the document (please go to question 5).

**NO** Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed (please complete questions 3 and 4)

**3. Details of the Data Subject (if different to 1)**

Full Name .....

Address .....

.....

Telephone Number ..... Fax Number .....

Email .....

**4. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.**

.....

.....

.....

**5. If you wish to see only certain specific document(s), for example a particular examination report, a specific departmental file, etc, please describe these below:**

.....

.....

**7. If you would like a more general search, please note that the University will normally automatically search the following sections for personal data:**

Registry, Library, Residences Office, Finance Office, College Office, Information Systems Services and any academic unit that you have studied with as part of your degree. *Please tick below any other sections/departments that you have been in contact with which you would like to be searched for relevant data.*

Section	Search
Student Union	
Advice and Information Service	
Careers Service	
Childcare Service	
Counselling Service	
Disability and Dyslexia Support	
Student Occupational Health	
Student Fees & Bursaries	
Chaplaincy	
Other(s). Please specify below	
<p>(1) Personal data processed if you have made an official complaint about e.g. standard of residence room, launderette, etc.</p> <p>(2) If CCTV search wanted please specify date(s) and time(s) and location (please note CCTV only kept for 28 days)</p>	

**Declaration**

I....., certify that the information given on this application form to London Metropolitan University is true. I understand that it is necessary for the University to confirm my/Data Subject's identity and that it may be necessary to obtain more detailed information in order to validate this request and locate the correct information.

Signed \_\_\_\_\_ Date.....

Please return the completed form to Peter Fisher, Room 80A, 2<sup>nd</sup> Floor, 31 Jewry Street, London, EC3N 2EY. Documents which must accompany this application are:

- i evidence of your identity
- ii evidence of the Data Subject's identity (if different from above)
- iii evidence of Data Subject's consent to disclose to a third party (if required as indicated above)
- iv where appropriate, a fee of £10 (cheques to be made payable to London Metropolitan University)
- v stamped, addressed envelope for return of proof of identity/authority documents, where appropriate

Please note that the University reserves the right to obscure or suppress information that relates to other third parties (under the terms of Section 7 of the Data Protection Act 1998).

**Office Use Only**

Request received .....

Date completed.....

Notes .....

.....

.....

## **General Comments**

The CCTV Policy Statement gives far more information than is required under the Data Protection Act as a legal requirement or as good practice!

Some of the suggested changes to the CCTV Policy Statement have been made without sight or knowledge of the 'procedures set out in the Procedures Manual' referred to in paragraph 5.2.

Appendix 1 refers to access to the Communications Centre. We are unsure as to the nature of the Communications Centre and are therefore unable to comment in this matter.

The Subject Access Request Form with regard to numbers 5 and 6 should also be related to the Freedom of Information Act. It should be further noted that, where information does not receive precedent under the Data Protection Act, the Freedom of Information Act includes for different response times by which a request must be replied to and different fees that may be charged.