



---

## INSTITUTE OF EDUCATION – CCTV POLICY STATEMENT OCTOBER 2011 to AUGUST 2012

---

### 1. Ownership:

- 1.1 The Institute of Education has in place a Closed Circuit Television (CCTV) system covering internally and externally the Institute's 20 Bedford Way premises, 10 to 18 and 24-28 Woburn Square, 55-59 Gordon Square, 15-23 Endsleigh Street and 9-11 Endsleigh Gardens. The system is owned by the Institute of Education – University of London – 20 Bedford Way – London – WC1H 0AL and is covered by the Data Protection Act 1998 under the Institute's Data Protection registration reference number Z6020689. Images from all cameras' are constantly being recorded and will be used in strict accordance with this policy.
- 1.2 The Institute's Head of Estates and Facilities (who may be contacted as detailed below) is responsible for the operation and management of the CCTV system and for ensuring compliance with this policy and the procedures which accompany it.

Head of Estates and Facilities	Anthony Tyrrell
Tel:	020 7612 6110
Mobile:	077 6817 5890
E-mail:	<a href="mailto:a.tyrrell@ioe.ac.uk">a.tyrrell@ioe.ac.uk</a>

In addition to the above, the Institute's manned security contractor who is engaged to provide contracted security staff also has operational responsibility for the CCTV system via their access to and monitoring of the screen from within the office located behind the Level 4 reception desk at Bedford Way.

LUPC Site Manager	Phil Carruthers
Tel:	020 8690 1903
Mobile:	079 4418 9147
E-mail:	<a href="mailto:philc@cis-security.co.uk">philc@cis-security.co.uk</a>

### 2. Data Protection Act 1998:

- 2.1 CCTV images which show a recognizable person, is Personal Data and is therefore covered by the Data Protection Act 1998. This policy is associated with the Institute's Data Protection Policy, the provision of which shall be adhered to at all times.

2.2 The Institute's Data Protection Officer responsible for the Institute's Data Protection Policy is:

Pro-Director: Strategy and Organisation

Steve Denton

Tel: 020 7612 6012  
E-mail: [s.denton@ioe.ac.uk](mailto:s.denton@ioe.ac.uk)

### **3. The CCTV system installed:**

- 3.1 The system installed comprises fixed position cameras, Pan Tilt and Zoom (PTZ) cameras, monitors, recording equipment and public information signs.
- 3.2 Cameras are located at strategic points principally the entrance and exits to buildings, foyer areas, lift lobbies, the library, IT server rooms, and the Students' Union. No cameras are positioned so as to be hidden from view and none focus on frontages or rear areas of known private accommodation.
- 3.3 CCTV signage has been prominently displayed at strategic entrance and exit points to the Institute's buildings where CCTV is in operation to inform, staff, students, visitors, contractors, members of the public etc. that CCTV is in operation, complete with details of who to contact in case of a query.
- 3.4 Whilst the system installed has been designed to enhance security of the Institute's buildings and its surrounds, it is not possible for the Institute to guarantee that the system will detect every incident and or provide sufficient evidence of every incident taking place within the areas under surveillance.

### **4. Purpose of the CCTV systems:**

- 4.1 The system installed at the Institute is for the primary purpose of ensuring the protection and safety of Institute property, staff, students and visitors while consistent with respect for individual's privacy and to monitor the movement of people entering and exiting Institute building's..These purposes will be achieved by monitoring the system to:
  - Deter those having criminal intent
  - Assist in the prevention and detection of crime
  - Facilitate the identification, apprehension and possible prosecution of offenders in relation to crime and anti-social behaviour.
  - Verify in the case of contracted staff, i.e. (but not limited to) security, cleaning staff etc. the times they may enter and leave the Institute's buildings as a means of monitoring contract compliance. This is because a situation may arise whereby there was reason to believe that contracted hours were either not being

adhered to or were being altered without mutual agreement.

The CCTV system as installed will not be used:

- To provide recorded images for publication on the world-wide web and or any other publication medium issued by the Institute.
- To record any sound as part of the system recordings.
- To perform covert recording as standard operational procedures.
- To monitor Institute of Education staff attendance.

## **5. Covert recording:**

5.1 Convert recording may only be used in the following circumstances on the written authorization and or request of the Institute's Pro-Director Strategy and Organisation where it has been assessed by at least one further member of the Institute's Senior Leadership Team as listed under Appendix One following discussion with the Institute's Head of Estates and Facilities.

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

5.2 Where covert recording is sanctioned it 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 specified suspected unauthorized activity.

5.3 Convert recording will only proceed following receipt of a detailed written request and written approval that confirms the need to use covert recording was considered and confirmed and acceptable.

## **6. Control Rooms / Viewing areas:**

6.1 Images captured by the CCTV system will be recorded on central servers located within the Institute's 20 Bedford Way, 55-59 Gordon Square and 15-23 Endsleigh Street premises. Images from both internal and external camera's will be viewed as real-time images only on monitors located at the Level 4 reception office 20 Bedford Way, reception office 15-23 Endsleigh Street and within the Head of Estates and Facilities office Room 522, 20 Bedford Way. The monitors viewing these images are not visible outside of the areas in which they are located.

6.2 No unauthorized access to the server's locations will be permitted at any time. Access will be strictly limited to authorized members of the Institute's Senior Leadership Team (as listed under Appendix One), the Institute's Head of Estates and Facilities, operational management working for CIS Security Limited and

maintenance engineers working for Philton Fire and Security Limited (the systems maintenance provider).

- 6.3 Access to the Level 4 reception office will be strictly limited to those named persons as detailed under Appendix 2 unless prior authorization from the Institute's Head of Estates and Facilities has been obtained.
- 6.4 In cases where it maybe necessary to allow other persons into the Level 4 reception office, those staff within the office will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. Where visitors are permitted a detailed log will be maintained which includes their name, their department or organisation they represent, the person who granted authorisation, times of entry and exit and purpose of the visit.

## **7. Administration and Procedures:**

- 7.1 It is recognized that images are sensitive material and subject to the provisions of the Data Protection Act 1998; the Institute's Pro-Director Strategy and Organisation is responsible for ensuring day to day compliance with the Act. Where it becomes necessary for images to be burnt to CD-Rom these will be handled in strict accordance with this policy and the procedures set out in Appendix A.19.6 "Security Systems – CCTV" of the Institute's Security Assignment Instructions.

## **8. Staff with access to the CCTV system:**

- 8.1 Staff working in or with authorised access to the Level 4 reception office 20 Bedford Way and reception office 15 to 23 Endsleigh Street will be made aware that the Institute is recording CCTV images. The Institute's Head of Estates and Facilities will ensure that staff authorised access to these area are fully briefed and trained in respect to functions, operation and administrative duties arising from the use of the CCTV system.

## **9. Recording:**

- 9.1 The CCTV installed at the Institute's premises uses digital recording technologies only. Recordings are made directly to hard disc which will be automatically over-written every twenty-one days.
- 9.2 The systems hard discs will only be replaced should they become damaged or inoperable.

## **10. Access to CCTV images:**

- 10.1 Access to digital recordings will be recorded in the Access Log Book as specified in the Section titled "CCTV recording and viewing equipment" of the Institute's Security Assignment Instructions.

- 10.2 Access to digital recordings will be restricted to those staff needing to have access in accordance with the purposes of managing the system as detailed under Appendix 3.
- 10.3 Disclosure of recorded material will only be made to third parties in strict accordance with the purpose of the system and is strictly limited to the following authorities:
- Law enforcement agencies where images recorded would assist in a criminal enquiry and or the prevention of terrorism and or disorder.
  - Relevant legal representatives
  - The media (at the request of the Police) where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
  - 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.

## **11. Access to Images by a subject:**

- 11.1 Digital recordings showing a recognizable person is Personal Data as defined under the Data Protection Act 1998. Anyone believing they have been filmed by the system installed at the Institute's premises is entitled to ask for a copy of the images recorded, subject to the prohibitions on access also covered by the Data Protection Act. They do not have the right of instant access but must abide by the Institute's Data Protection procedures.
- 11.2 As the Institute's system uses digital recordings, CD-ROMs can be provided as long as no third parties can be seen. If a third party can be seen then still images of the person requesting the access will be provided but only with all other third party images masked.
- 11.3 A person whose image has been recorded and retained and who wishes access to the recording must apply in the writing to the Institute's Data Protection Officer. Access request forms are available on request from the Pro-Director Strategy and Operations. Submission of the form must be accompanied by a fee of ten pounds (£10.00).
- 11.4 Upon receipt of an Access request form, the Data Protection Officer will then arrange for a copy of the recording to be made and given 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 recording. All communications must go through the Institute's Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.
- 11.5 The Data Protection Act gives the Institute's Data Protection Officer the right to

refuse a request for a copy of the recording particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

11.6 All Access Requests received will be referred to the Head of Estates and Facilities by the Data Protection Officer.

11.7 If it is decided that an Access Request is not to be complied with, the reasons will be fully documented and the applicant informed, in writing stating the reasons.

## **12. Request to prevent access to images:**

12.1 An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage to that individual.

12.2 All such requests should be addressed in the first instance to the Institute's Head of Estates and Facilities or 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.

## **13. Complaints:**

13.1 It is recognized that Institute employees, students and visitors may have concerns and or complaints about the operation of the CCTV system. Any concerns and or complaints should be addressed in the first instance to the Institute's Head of Estates and Facilities. An acknowledgement e-mail will be sent to confirm receipt. Concerns and or complaints will be investigated and formally responded to within twenty-one working days. Should the concern and or complaint take longer than this time period to investigate or address, periodic updates will be forwarded.

13.2 Concerns and or queries relating to the provision of the Data Protection Act 1998 may be addressed to the Institute's Data Protection Officer Steve Denton e-mail: [s.denton@ioe.ac.uk](mailto:s.denton@ioe.ac.uk).

13.3 These rights do not alter the rights of staff and or students under any relevant grievance or disciplinary procedures.

## **14. Compliance monitoring:**

14.1 The contact point for Institute staff, students, visitors or members of the public wishing to enquire about the system will be the Institute's Head of Estates and Manager and is contactable between the hours of 09:30 to 16:30 Monday to Friday except public holidays and days when the Institute is official closed. During his/her absence enquiries can directed to the Institute's Director of Finance and Estates Services.

14.2 Upon request enquirers will be provided with:

- A copy of this policy
- An Access Request Form if required or requested
- A copy of the CCTV operational procedures

14.3 All documented procedures relating to the operation and management of the CCTV system will be kept under periodical review and the Institute's Safety and Security Committee will be kept informed of changes in operational procedures.

14.4 The effectiveness of the CCTV system in meetings its purpose will be kept under review and reports submitted as required to the Institute's Safety and Security Committee.

**This policy has been updated on: 11 October 2011**

## **Appendix 1**

Institute's Senior Leadership Team permitted to access in conjunction with the Institute's Head of Estates and Facilities a request for covert recording.

Director  
Pro Director Strategy and Operations  
Academic Registrar  
Head of Human Resources and Staff Development  
Head of Marketing and Communications

## **Appendix 2**

Those authorized to have access to view real-time images.

Director  
Pro Director Strategy and Operations  
Director of Finance and Estates  
Academic Registrar  
Head of Human Resources and Staff Development  
Head of Marketing and Communications  
Internal Auditor  
Students' Union General Manager  
Students' Union Commercial Manager  
Head of Estates and Facilities  
Support Services Manager  
Support Services Assistants  
Head of Conference, Catering and Residences  
Residence Staff  
Technical Media Staff  
CIS Security Limited Security Officers assigned to the premises  
CIS Security Limited LUPC Site Manager  
CIS Security Limited Regional Contracts Manager  
Philton Fire and Security Limited engineers attending maintenance

## **Appendix 3**

Those authorised to have access to hard drives for the purposes of searching and reviewing images and recording to CD-Rom for evidence purposes.

Director  
Pro Director Strategy and Operations  
Head of Estates and Facilities  
Network Operating System Analyst  
CIS Security Limited LUPC Site Manager (following authorization from Head of Estates and Facilities)