London South Bank University

EST 1892

CCTV Policy

Policy last reviewed	November 2018
Approved by	Chief Business Officer, Deputy Vice Chancellor Innovation
If you have any questions about this policy, please contact:	Head of Security and Estates Customer Services; OR Data Protection and Information Compliance Officer

This procedure is available in accessible format on request from the Head of Security and Estates Customer Services at security-office@lsbu.ac.uk

Table of Contents

1. Policy statement

1.1. This Policy seeks to ensure that the Close Circuit Television (CCTV) system used at London South Bank University (LSBU) is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018")) and includes the principles governing the processing of personal data as set out in Appendix 1. It also seeks to ensure compliance with privacy law. It takes into account best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office. LSBU therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 1.2, and only if it is proportionate to that aim.

1.2. LSBU seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property and premises. LSBU therefore deploys CCTV to:

- promote a safe LSBU community and to monitor the safety and security of its premises;
- assist in the prevention, investigation and detection of crime;
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
- assist in the investigation of breaches of its codes of conduct and policies by staff, students and contractors and where relevant and appropriate investigating complaints.

1.3 This policy will be reviewed annually by the Head of Security & Estates Customer Service to assess compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV system remains justified.

1.4 The operational requirements for the CCTV system in use across LSBU are documented in a "CCTV Operational Requirement Report", held and maintained by the Head of Security & Estates Customer Service.

2. Scope

2.1 This policy applies to CCTV systems in all parts of LSBU's Southwark and Havering campuses and to the Halls of Residences.

2.2 This policy does not apply to any Webcam systems located in meeting rooms or lecture theatres operated by Schools or ICT, which are used for the purposes of monitoring room usage and to assist with the use of the audiovisual equipment.

2.3 This policy applies to all LSBU staff, contractors and agents who operate, or supervise the operation of, the CCTV system including Security Management

and Staff, Academy of Sport Management, Halls of Residences Management and the Data Protection and Information Compliance Officer.

3. Roles and Responsibilities

3.1 Chief Business Officer, Deputy Vice Chancellor Innovation has the overall responsibility for this policy, but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.

3.2 The Head of Security & Estates Customer Service is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 1.1 of this policy. Where new surveillance systems are proposed, the Head of Security & Estates Customer Service will consult with the Data Protection and Information Compliance Officer to determine whether a prior privacy impact assessment is required.

3.3 Only the appointed Estates and Academic Environment Department maintenance contractor for LSBU's CCTV system is authorised to install and/or maintain it.

3.4 The Head of Security & Estates Customer Service is responsible for the evaluation of locations where live and historical CCTV images are available for viewing via the network software. The list of such locations and the list of persons authorised to view CCTV images is maintained by the Head of Security & Estates Customer Service.

3.5 Changes in the use of LSBU's CCTV system can be implemented only in consultation with LSBU's Data Protection and Information Compliance Officer or the University Solicitor.

4. System description

4.1 The CCTV systems installed in and around LSBU's estate cover building entrances, car parks, perimeters, external areas such as courtyards, internal areas such as social spaces, computer rooms, rooms with high value equipment, some corridors and reception areas. They continuously record activities in these areas and some of the cameras are set to motion detection.

4.2 CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc.

4.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, students, visitors and members of the public are made aware that they are entering an area

covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

4.4 The contact point indicated on the CCTV signs around LSBU should be available to members of the public during normal business hours. Employees staffing the contact telephone number point must be familiar with this document and the procedures to be followed in the event that an access request is received from a Data Subject or a third party.

5. Covert recording

5.1 Covert recoding (i.e. recording which takes place without the individual's knowledge):

5.1.1 may only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e. there is no other reasonable, less intrusive means of achieving those purposes;

5.1.2 may not be undertaken without the prior written authorisation of the Director of People and Organisation or in their absence, the Chief Business Officer, Deputy Vice Chancellor Innovation at the request of the Head of department/Dean or in their absence their Deputy or nominee. All decisions to engage in covert recording will be documented, including the reasons;

5.1.3 will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted; and

5.1.4 will only be carried out for a limited and reasonable period consistent with particular purpose of the recording and will not continue after the investigation is completed.

6. Operating Standards

6.1 The operation of the CCTV system will be conducted in accordance with this policy.

6.2 Control room

6.2.1 No unauthorised access to the Security Control Room ("the Control Room") will be permitted at any time.

6.2.2 Other than Security Control Room Staff, access to the Control Room will be limited to:

- persons specifically authorised by the Head of Security;
- security Operations Manager;
- security Supervisor;
- security Control Room Operator;
- maintenance engineers;
- police officers where appropriate; and
- any other person with statutory powers of entry.

6.2.3 Monitors are not visible from outside the Control Room.

6.2.4 Before permitting access to the Control Room, security staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. All visitors are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the person who granted authorisation and the times of entry to and exit from the Control Room. A log of shall be retained setting out the following:

- person reviewing recorded footage;
- time, date and location of footage being reviewed; and
- purpose of reviewing the recordings.

6.3 Processing of Recorded Images

6.3.1 CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

6.4 Quality of Recorded Images

6.4.1 Images produced by the recording equipment must be as clear as possible so they are effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to at clause 1 of these procedures are set out below:

- recording features such as the location of the camera and/or date and time reference must be accurate and maintained;
- cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established;
- consideration must be given to the physical conditions in which the

cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;

- cameras must be properly maintained and serviced to ensure that clear images are recorded and a log of all maintenance activities kept; and
- as far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

6.5 Retention and Disposal

6.5.1 CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce an approximate 28-day rotation in data retention.

6.5.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

6.5.3 All retained CCTV images will be stored securely.

7. Data Subject Rights

7.1 Recorded images, if sufficiently clear, are considered to be the personal data of the individuals (Data Subjects) whose images have been recorded by the CCTV system.

7.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

7.3 Data Subjects can exercise their rights by submitting a request to the Data Protection and Information Compliance Officer in the form contained in Appendix 2 along with evidence of their identity.

7.4 On receipt of the request, the Data Protection and Information Compliance Officer will liaise with the Head of Security and Estates Customer Service regarding compliance with the request, and subject to clause 7.5, the Data Protection and Information Compliance Officer will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

7.5 The period for responding to the request may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Data Protection and Information Compliance Officer will notify the Data Subject of any such extension within one month of receipt of the request together with reasons.

8. Third Party Access

8.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:

- legal representative of the Data Subject;
- law enforcement agencies including the Police;
- disclosure required by law or made in connection with legal proceedings; and
- HR staff responsible for employees and university administrative staff responsible for students in disciplinary and complaints investigations and related proceedings .

8.2 Legal representatives of the Data Subjects are required to submit to LSBU a letter of authority to act on behalf of the Data Subject and the subject access request form (please see Appendix 2) together with the evidence of the Data Subject's identity.

8.3 The Data Protection and Information Compliance Officer will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either: an investigation concerning national security; the prevention or detection of crime; or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

8.4 Every disclosure of CCTV images is recorded in the CCTV Operating Log Book and contains:

- the name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording;
- brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy;
- the crime reference number where relevant; and
- date and time the images were handed over to the police or other body/agency.

8.5 Requests of for CCTV images for staff or student disciplinary purposes (or complaints purposes) must be authorised by HR Business Partners or Student

Disciplinary Officer respectively and by the Head of Security & Estates Customer Service in consultation with the Data Protection and Information Compliance Officer.

8.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

9. Complaints Procedure

9.1 Any complaints relating to the CCTV system should be directed in writing to the Head of Security & Estates Customer Service promptly and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office. If a complainant is not satisfied with the response they may appeal to the Director of Estates and Academic Environment.

9.2 Complaints in relation to the release of images should be addressed to the University Secretary and Clerk to the Board of Governors as soon as possible and in any event no later than three months from the event giving rise to the complaint

10. Useful links

The Information Commissioner's Code of Practice can be found at:
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

The Home Office Code can be found at:
https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

Appendix 1

Principles relating to the processing of personal data under the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Appendix 2

Request to Disclose Personal Data Form

Data Protection Contact Details	Email:	dpa@lsbu.ac.uk
	Tel:	020 7815 7815
	Website:	http://www.lsbu.ac.uk/footer/data-protection
LSBU-ICO Reference#	Z6533032	
Request Number: (LSBU use only)		

Under data protection legislation (General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018)) London South Bank University (LSBU) must process personal data lawfully, fairly, transparently and for specified purposes (and not further processed in a way that's incompatible with those purposes).

Exemptions apply which allow LSBU to process (including disclosing) personal data in certain circumstances. However, there must always be a legal basis for the processing. LSBU has compiled this form to support you in making your request for disclosure of personal data. Please complete all relevant sections, giving as much information as possible. We will use it to:

- help us identify the data subject(s) and personal data relevant to your request,
- determine as a data controller whether or not we are able to process/disclose the personal data, and
- document the request and provide an auditable trail.

Unless LSBU is satisfied that we are authorised to process the personal data by a legal basis in keeping with the data protection principles and data subject rights, or exemptions provided by the DPA 2018, we will be unable to disclose the personal data to you.

2. Details about the data subject

Full name:			
Address: *(if relevant)*			
Previous address: *(if relevant)*			
Telephone number: *(if relevant)*			
Email address: *(if relevant)*			
Reference number: **(i.e. staff/student number)**	**Staff number:**		
	Student number:		
The data subject is a(n): *(please tick whichever apply)*	**applicant or prospective student**		
	student or former student (including alumni)		
	employee or former employee (or contractor)		
	customer or other stakeholder		
Any other information to enable identification of the individual?			

3. Your details as a requester (if you are external to LSBU)

Full name:	
Organisation:	
Role within your organisation:	
Email address:	
Telephone number:	

4. Your details as a requester (if you are an employee/ contractor of LSBU)

Full name:	
Position held:	
Department/School: *(where applicable)*	
Line manager/School Dean: *(where applicable)*	
Email address:	
Telephone/extension number:	

5. Legal basis for processing and applicable exemptions

All processing of personal data must have a legal basis. Please describe which bases apply to this request:	
Consent of the data subject	
Performance of a contract	
Comply with a legal obligation	
Protect vital interests	
Performance of a public task or exercise of official authority	
Legitimate interests	

If you are requesting special category data, please specify the additional legal basis you are relying on (or exemptions in the Data Protection Act 2018): *(Mainly see Schedule 1 of the Data Protection Act 2018)*

If you are relying on exemptions in the Data Protection Act 2018 for the disclosure of personal data, please specify which exemptions: *(Mainly see Schedules 2-4 of the Data Protection Act 2018)*
If non-disclosure would be likely to prejudice the purposes for which you are requesting disclosure of personal data, please explain:

6. Details relating to the personal data you are requesting

Please include as much information as possible to helps us identify the personal data you're requesting.			
The personal data requested covers the following dates.			
From:		To:	

7. Signatures

Signature:		**Dated:**	
Position/Role:			
Counter signature: *(e.g. manager, HR rep, etc.)*		**Dated:**	
Position/Role:			

*You can complete this form electronically and send it to dpa@lsbu.ac.uk, or manually and scan it to the same email address. Should you wish to mail the form, the address is:

Data Protection and Information Compliance Officer,
Governance, Information and Legal Team,
London South Bank University,
103 Borough Road,
London SE1 0AA.

London
South Bank
University

EST 1892