Surveillance Technology and Access Control Policy

Document type:	Policy		
Document number:	EST-011	**Version**	02
Department:	Estates		
Approved by:	Executive Board		
Date approved:	25/11/2024	**Review Date**	25/11/2027
Publication:	SOAS website		

Note: All policies must be read in conjunction with all other SOAS policy, procedure and guidance documents. Printed copies of policies may not be the most up to date, therefore please refer to the policy pages on the SOAS external website or intranet for the latest version.

1. Introduction / Purpose

1.1 This policy sets the framework for SOAS' deployment and use of Surveillance Technology and Access Control. Surveillance Technology is installed and operated across the campus to ensure the safety and security of students, staff and visitors. CCTV acts as a deterrent to anyone intending to commit a crime against person or property on campus, whilst access control logs help us understand who is on campus at any particular time for broader health, safety and security purposes. Records derived from CCTV, other surveillance technologies such as Body Worn Video, and Access Control systems can be used as a source of evidence should the university need to investigate incidents on campus.

Whilst Surveillance Technology is a critical component of campus safety and security measures, we must ensure that, in order to build and maintain trust in its use within our community and amongst the public, we only deploy the technology in a way that is fair to all and transparent. The Surveillance Technology and Access Control Policy explains how we will achieve this objective.

This policy must be read in conjunction with the *Surveillance Technology and Access Control Procedure.*

2. Scope of Policy

2.1 This policy sets the framework for SOAS' deployment and use of Surveillance Technology and Access Control. Surveillance Technology is installed and operated across the campus to ensure the safety and security of students, staff and visitors

2.2. This policy covers the use of Surveillance Technology and Access Control systems at SOAS which record and store personal data about students, staff, contractors and visitors on our campus where SOAS is the Data Controller in respect of this personal data. This Policy conforms to the provisions set out in *SOAS's Data Protection Policy*.

2.3 This policy is designed to be consistent with the Information Commissioner's Office's (ICO) Guidance on Video Surveillance

3. Definitions

- **Access Control** is defined as any device or system which captures information about an individual's access to or exit from any building, facility or room on campus.
- **Body Worn Video** is defined as a device worn by Campus Safety staff with the capability to record video and sound.
- **CCTV** is defined as static closed circuit television cameras which record images, but not sound.
- **Contractors** is defined as any individual who is contracted to a company providing services to the university
- **Staff** is defined as any individual employed directly by the university.
- **Surveillance Technology** is defined as any device or system that captures video and/or audio of individuals or relating to individuals. The term is used throughout this policy to refer to any technology with audio/video recording capabilities which is used for safety and security purposes, and includes CCTV and Body Worn Video
- **Systems Data** is defined as information generated automatically from Surveillance Technology or Access Control and stored and managed on SOAS approved networks.
- **The Procedure** means the Surveillance Technology and Access Control Procedure

4. Roles and Responsibilities

4.1 The Estates and Property Services Directorate (hereafter "Estates Directorate") is responsible for the siting, positioning, maintenance and operation of Surveillance Technology and Access Control.

4.2 The Information & Technology Directorate is responsible for ensuring Surveillance Technology and Access Control can be reliably connected to the university network.

5. System Operation

5.1 SOAS operates Surveillance Technology and Access Control to protect staff, students, contractors and visitors, and to facilitate compliance with health and safety regulations.

5. 2 The Estates Directorate will decide where to install CCTV and Access Control devices and will make such decisions in conformance with British Standards. Cameras will be visible, and located in positions that minimise viewing of spaces that are not relevant for the maintenance of security and health and safety at SOAS. In particular, cameras will not be sited to capture images of areas where individuals would have heightened expectations of privacy, for example in or around toilet or changing facilities.

5.3 The Estates Directorate will keep and maintain a Data Protection Impact Assessment (DPIA) covering the operation of Surveillance Technology and use of recorded footage from Systems Data. The DPIA is an iterative process, and will be updated as and when substantive changes are made to the operation of Surveillance Technology at SOAS. The DPIA is informed by the ICO and Surveillance Camera Commissioner's (SCC) guidance for carrying out a DPIA on surveillance camera systems, and is based on the ICO/SCC template.

5.4 CCTV cameras are in continual use, and are monitored by approved staff 24 hours a day

5.5 Signs explaining that CCTV is in operation and providing a contact number and/or email address for queries or concerns will be placed prominently at the entrance to any building on campus in which CCTV is installed.

5. 6 SOAS will operate Surveillance Technology and use Systems Data with respect for the privacy of individuals and in accordance with applicable UK data protection legislation.

6. Processing

6.1 SOAS maintains a Record of Processing Activity (ROPA) which records the purpose for processing surveillance footage and access control logs, lawful basis for processing personal data, and Article 9 condition for processing Special Category or Criminal Offence Data, as well as the retention period. Personal data processed in Systems Data is included in the Security and CCTV ROPA.

6.2 The university has the right to use Systems Data for evidential purposes where the information is necessary to support an investigation into a health, safety and security incident or a case under the relevant *Student Complaints* and *Disciplinary Procedures* or *Staff Grievance* and *Disciplinary Procedures.*

7. Data Subject Access Requests (DSARs)

7.1 Individuals have the right to make a request for information in Systems Data which relates to themselves. Requests for the disclosure of personal data in Surveillance Technology recordings or Access Control logs will be managed and authorised by the SOAS Information Compliance Manager.

7.2 DSARs for personal data in Surveillance Technology recordings or Access Control logs can be made in accordance with our *Guidance on Requesting Access to Personal Data*

8. Other Access Requests

8.1 Routine access to Systems Data will be restricted to authorised members of staff who are responsible for operating and maintaining Surveillance Technology and Access Control. This includes Campus Safety personnel and members of the Information & Technology infrastructure team.

8.2 Requests from external parties for a copy of footage from Surveillance Technology must be made in writing to the Information Compliance Manager at dataprotection@soas.ac.uk. Requests from authorities exercising a law enforcement function must be made using their standard forms and explain the purpose for which the footage is required, why the disclosure is necessary to achieve the purpose, and citing the relevant provisions in the Data Protection Act (2018).

8.3 Requests from university staff for a copy of footage from Surveillance Technology must be made in writing to campussafety@soas.ac.uk. The Campus Safety team will follow the process outlined in section 6 and Appendix A of The Procedure.

8.4 Requests made by authorities exercising a law enforcement function to view footage on campus in an emergency or time sensitive situation will be permitted to do so within SOAS security offices/control rooms, under the supervision of SOAS Campus Safety staff, subject to authorisation by the Assistant Director of Campus Safety or their delegate. SOAS' Safety Team will ensure the form in Appendix B of The Procedure is completed.

8.5 From time to time SOAS Contractors may have access to Systems Data when carrying out their contracted services to the university. SOAS' agreements stipulate that Contractors must have adequate data protection training and include protective clauses covering personal data and/or confidential information.

8.6 SOAS will keep a record of requests to access footage and any decision made by the university in response to such a request.

9. Retention

9.1 SOAS will retain footage recorded from CCTV for 30 days from the date of recording

9.2 SOAS will retain Access Control logs for 6 months from the date the log is generated

9.3 SOAS will retain Body Worn Video footage for no longer than 72 hours from the date of recording

9.4 Notwithstanding the retention periods stated in 5.17 to 5.19, Systems Data which is needed as evidence to support an investigation will be retained for six years after the date on which the investigation is closed or concludes.

10. Security

10.1 SOAS will ensure appropriate technical and organisational measures are in place to protect Systems Data from unauthorised or accidental loss, disclosure, alteration or corruption.

10.2 Staff responsible for the operational processing of personal data in Systems Data or handling Systems Data as evidence for investigatory purposes will be trained to use the relevant technology safely and effectively, and will have received training on protecting personal data.

10.3 Screens used to monitor live footage from CCTV will never be visible to the public, and will be located in secure offices or control rooms on campus.

11. Audit

11.1 The Estates Directorate is responsible for auditing the site and location of CCTV on campus to ensure the coverage meets, but does not exceed, the university's requirements.

11.2 Checks of CCTV equipment and software will be carried out to ensure that they are functioning properly. Where date, time and system overlays are used, annual checks will ensure that these are accurate. A record will be kept of all such checks.