Surveillance Technology and Access Control Procedure

Document type:	Policy		
Document number:	EST-12	**Version**	01
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. Purpose and Scope

1.1. This procedure supports the Surveillance Technology and Access Control Policy and sets a framework for the operation of the systems and use of the data in records created and stored by them.

1.2. This procedure is designed to ensure SOAS is able to meet the requirements of the *Surveillance Technology and Access Control Policy*.

1.3. This procedure is designed to ensure SOAS' use of Surveillance Technology and Access Control complies with our legal obligation to respect individuals' right to privacy.

1.4. This procedure is written in accordance with the Information Commissioner's Office Code of Practice on the use of personal data in surveillance systems, acknowledging that the university is the Data Controller for personal data recorded by Surveillance Technology and Access Control on university premises.

2. 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 members of the Safety Team with the capability to record video and sound.
- **CCTV** is defined as static closed circuit television cameras which record images, but not sound.

- **Data Protection Legislation** means the UK Data Protection Act (2018) (DPA) and the UK General Data Protection Regulation (UK GDPR) as defined in section 3 (10) of the DPA, and any successor regulations or legislation.
- **Data Subject, Data Controller, Processing** have the meaning given in the Data Protection Legislation
- **ICO Code** is the Information Commissioner's Office Code of Practice on the use of personal data in surveillance systems (2017)
- **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 procedure to refer to any technology with audio/video recording capabilities which is used for safety and security purposes, and includes CCTV and Body Warn Video
- **Systems Data** is defined as information generated automatically from Surveillance Technology or Access Control and stored and managed on SOAS approved networks.

3. Personal Data Processing in Systems Data

3.1 The lawful basis under Article 6 of the UK GDPR for processing personal data contained in Systems Data records is Legitimate Interests. In the event SOAS' Surveillance Technology captures Criminal Offence Data, this processing is authorised by law in accordance with Article 10 of the UK GDPR and Schedule 1, Part 2, paragraph 10 of the UK Data Protection Act. In the event SOAS' Surveillance Technology captures Special Category Data, this processing is authorised by law in accordance with Article 9 of the UK GDPR and Schedule 1, Part 2, paragraph 8 of the UK Data Protection Act. SOAS will operate Surveillance Technology in a manner consistent with our Data Protection Policy and Data Protection Legislation.

3.2 There is a high probability that all Systems Data will contain personal data, and SOAS is committed to keeping this data secure and only for as long as necessary in accordance with our university policies.

3.3 External parties may request access to Systems Data, particularly CCTV footage, in specific circumstances. Systems Data may also be shared internally with university staff, such as People Services or Student Casework, to support investigations under university procedures.

4. Video Surveillance

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

4.2 To achieve the university's objective of protecting the SOAS community, Surveillance Technology is deployed for the following, non-exhaustive, list of purposes:

- To assist in the prevention and detection of crime or the identification, apprehension and prosecution of offenders
- To assist in the identification of actions which might result in disciplinary proceedings
- To monitor security of campus buildings
- To manage events
- To identify vehicle movement issues around campus

4.3 When SOAS introduces new Surveillance Technology on campus, the ICO Code will be followed. The Code recommends the responsible body follows these steps prior to installing cameras or introducing other Surveillance Technology:

- We have identified the purpose for the technology and the problem we are trying to address
- Cameras produce clear images which can easily be downloaded and shared with third parties in specific circumstances (e.g. law enforcement agencies)
- We have positioned cameras in a way to avoid unintentional capture of private land or individuals not visiting the premises (which includes the precinct between SOAS buildings)
- We display visible signs at building entry points to show that CCTV is operational. The signage includes contact information.
- We have added the deployment of any additional surveillance technology to our Data Protection Impact Assessment in order to identify and address any new or escalated existing risks resulting from the additional deployment.

4.4 CCTV is continually monitored by university members of the Campus Safety Team within the Estates Directorate. Staff responsible for monitoring CCTV footage must have passed SOAS' mandatory Information Security and Data Protection training, and be trained in the use of the technology.

4.5 SOAS' use of its CCTV system will not involve:

- Streaming footage to publicly viewable monitors on campus, to the university intranet, or to the internet
- Recording audio alongside images
- Disclosing footage to the media unless in co-operation with a public appeal during a police investigation

5. Disclosure requests from individuals

5.1 Anyone whose data is recorded in Systems Data can ask for a copy of their data under UK data protection law.

5.2 Guidance on making a request for personal data is available on the SOAS website: *Requesting access to personal data*

5.3 SOAS requires sufficient information from the Data Subject to enable us to make a reasonable search for their personal data. Consequently, when requesting personal data from CCTV footage, an individual must provide us with:

- Sufficient information to verify their identity in the footage
- The date and time the images were recorded
- The precise location of the camera and/or the specific area of campus where they believe footage may have been recorded

5.4 Personal data in CCTV footage is likely to comprise 'mixed personal data' (i.e. information about the individual in addition to other members of the community/public). The university Data Protection Officer will assess the risk to the privacy of third parties and will decide whether the right to access is best satisfied by disclosing a copy of the recording to the individual, by arranging a viewing session on campus, or by providing stills from the recorded footage.

5.5 The university reserves the right to refuse a request for access if the request cannot be satisfied in the manner outlined in 5.4 without infringing the privacy rights of third parties.

6. Disclosure requests from SOAS departments

6.1 SOAS may need to share Systems Data internally to support university procedures, in particular complaints made under our Student Complaints Procedure or Student Disciplinary Procedure, or our staff grievance or disciplinary procedures.

6.2 Any request for Systems Data from SOAS departments must be necessary to enable them to discharge their responsibilities to the university.

6.3 Colleagues who wish to access Surveillance technology footage must write to the Campus Safety Team at campussafety@soas.ac.uk. The request must include:

- The reason for requesting the footage
- The exact time and date of the footage
- The location of the incident/camera

6.4 The Campus Safety Team will progress the request according to the diagram in Appendix A

6.5 Where video footage from surveillance cameras is used as evidence in misconduct investigations and the footage includes identifiable individuals other than the respondent, the disclosure of footage to the respondent must only be carried out through an in person viewing on campus, and the investigating manager must take every precaution to ensure the footage is not recorded. If it is not possible to arrange a viewing on campus, the investigation manager must consult with the Information Compliance Office to find an alternative method of disclosing the evidence.

7. Disclosure requests from external parties

7.1 Disclosure requests from external parties will only be acted upon in accordance with the purposes of the technology and the prevailing data protection legislation. We may disclose Systems Data to:

- Law enforcement agencies, where the data is necessary to support a specific police enquiry or investigation, at the university's discretion
- A court or tribunal which has issued a binding order for the data
- Legal representatives where the data is necessary for the purpose of, or in connection with, legal proceedings; or to obtain legal advice; or to establish, exercise or defend a legal claim
- Other agencies or bodies with statutory powers to investigate and prosecute
- Other third parties where the needs of the third party outweigh the privacy rights of the data subject(s)

7.2 All requests from external parties for access to a copy of Systems Data must be made in writing to the Information Compliance Office at dataprotection@soas.ac.uk. If the request is from a law enforcement or prosecution agency, it should be made under UK Data Protection Law. If the request is sent to another office at the university, it should be redirected to the Information Compliance Office.

7.3 If Systems Data is needed by an external party to respond to an emergency situation, for instance where the health of any person is endangered, the data can be shared without following the authorisation process outlined in Appendix A to the extent that it is necessary and proportionate to do so.

7.4 The authorisation process for sharing Systems Data with Staff, Contractors or external parties is illustrated in Appendix A

7.5 The university must fully document requests for access to Systems Data received from external third parties. When a request to view or access a copy of Systems Data is received, the details will be logged in the Surveillance Tech request register in Sharepoint.

7.6 In some instances external parties may request access to view footage on campus shortly after an incident has occurred. These requests should be documented using the form in Appendix B, and should only be permitted where the viewing is a necessary and proportionate measure to achieve the objective. Notwithstanding the exception in 7.3 above, no copies of footage or other Systems Data can be removed from campus by a third party until the approval process in Appendix A has been followed.

8. Security

8.1 Systems Data will be stored on university approved servers which provide a level of protection proportionate to the level of risk associated with the data.

8.2 Systems Data will only be shared over a network with recipients approved under the terms of sections 5, 6 and 7 of this Procedure using technology which encrypts data in transit with the TLS 1.2 protocol as a minimum

8.3 Where Systems Data is shared on physical media, the data will be protected by a secure 12 character password which meets the requirements of SOAS' Password Policy.

9. Objections

9.1 Individuals have the right to object to their data being processed in SOAS's Surveillance Technology and Access Control systems, or to ask SOAS to restrict the processing of their data through these systems. To exercise these rights, an individual should write to dataprotection@soas.ac.uk, and the Information Compliance team will consider the request in consultation with the Estates Directorate.

10. Complaints

10.1 Complaints and feedback about the operation of Surveillance Technology and Access Control in SOAS buildings should be submitted to campussafety@soas.ac.uk.

11. Access Control Records

11.1 Access Control records contain the following information:

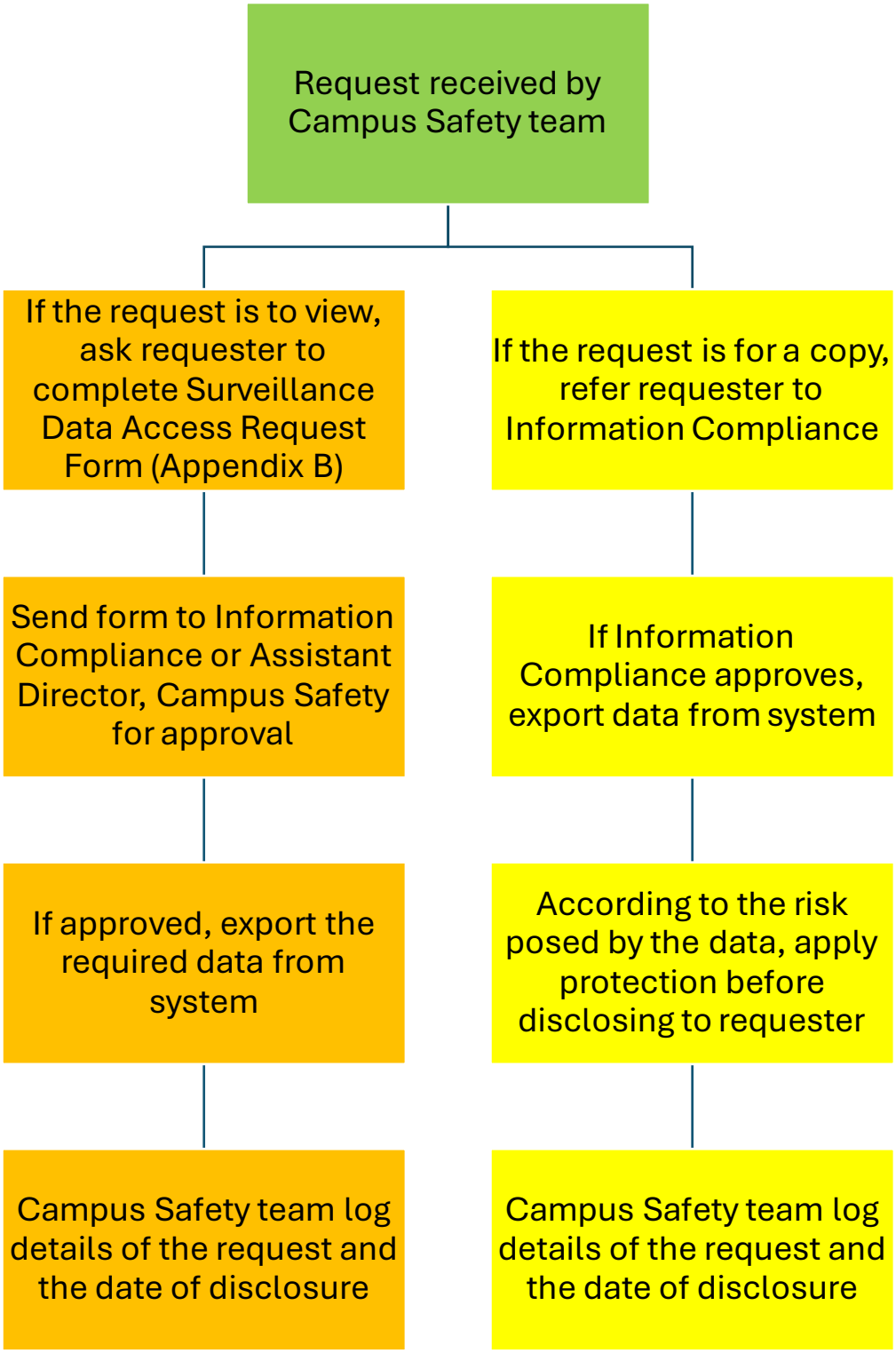
- Name
- ID
- Department
- Access clearance

11.2 Access Control records may be accessed by Staff and university contractors where necessary to perform their contracted roles. The groups with routine access to these records are:

- The Campus Safety Team, including the Assistant Director of Campus Safety
- IT support staff
- Library Readers Services staff (in respect of Library turnstiles)

11.3 Where data is released from the Access Control system, in compliance with the processes set out in this Procedure and where practically possible, all fields which make the data identifiable as belonging to a specific person should be removed. For example, if a request asks to know how many people used a reader during a certain period, the report need not include the names of the cardholders or any other personal information, just the quantity of card reads.

Appendix A: Authorisation process for requests for Surveillance Technology and Access Control data



Appendix B– Surveillance Data Access Request Form

Routine request to view Surveillance Technology footage/images
This form should be used for routine requests to view footage or images by individuals whose images have been captured and/or uniformed police on the same day or days immediately following an incident in order to, for example, assist in a specific criminal enquiry, or identify a victim, witness or perpetrator in relation to a criminal incident. It may also be used by other individuals whose data has not but captured but where they can demonstrate a strong legitimate interest in viewing the footage and the individual's rights override the privacy risks to any individual captured in the footage

This form should **not** be used where the police or other law enforcement agencies request a *copy* of footage or images. These requests should be made under the relevant Data Protection legislation for this type of access. Please refer to the Information Compliance team.

This form should **not** be used where an individual whose image has been recorded requests a *copy* of footage or images relating to themselves. A subject access request under the relevant data protection legislation is required for this type of access. Please refer to the Information Compliance team.

The form can be completed electronically or manually by the requester, or by a member of the Campus Safety Team on behalf of the requester. If you are requesting to view footage and completing the form yourself, either email it to campussafety@soas.ac.uk or hand it to a member of the Campus Safety Team.

To be completed by requester

Date	
Person making request	
Organisation	
Reason for request	
Crime reference number (if applicable)	

To be completed by member of staff supervising viewing

Reason for accepting request	
Reason for refusing request	
Camera reference, date and time of footage	
Name and signature	
CAD number	
Position	
Date	