Surveillance Camera System Procedure	
Enabling Policy Statement; Executive Owner; Approval Route:	Our Operations - Chief Operating Officer - Operations Committee
Associated Policy Statements:	Our Data
Authorised Owner:	Security Support Manager
Authorised Co-ordinator:	Head of Information Governance
Effective date:	18 July 2023
Due date for full review:	18 July 2026
Sub documentation:	There is no sub documentation to be added.

Approval History

Version	Reason for review	Approval Route	Date
1.0	The reason for this review is to update the current policy and migrate it to POPP.	Operations Committee	18 July 2023

1. Purpose

1.1. This procedure is informed by the "Our Operations Policy" in supporting its purpose and scope to "create the conditions for success through simple, effective and efficient delivery of the common services required by our institution".

1.2 The University's Surveillance Camera Systems (SCS) incorporates Closed-Circuit Television (CCTV), Body Worn Video (BWV) and covert means of recording images and audio. These are a powerful tool used by the Security Team to provide effective and efficient delivery of a service that deters and assists in the prevention of crime, monitoring security of buildings and assisting with efforts to enhance community safety on campus.

1.3 The framework for the operation of SCS at the University is provided by the Biometrics and Surveillance Camera Commissioner's updated Surveillance Code of Practice which laid before Parliament and came into effect on 12 January 2022 and is applied in the context of the University of Surrey through this SCS procedure.
Update to Surveillance Camera Code of Practice - GOV.UK (www.gov.uk)

2. Scope and Exceptions to the Procedure

2.1. All University of Surrey Security staff are subject to the SCS Procedure and are required to adhere to the application of this procedure.

2.2. The Director of Campus Services is accountable for the management of the SCS. Staff who have been designated as having responsibility for the management and the operation of the SCS are required to undertake their responsibilities strictly in accordance with this Procedure. They are required to operate the SCS fairly, within the law, and only for the objectives of preventing and deterring crime, securing property, providing evidence to be used in court and to help in providing a safe and secure campus for staff, students and visitors.

3. Definitions and Terminology

3.1. Any reference in this Procedure to CCTV (Closed Circuit Television), SCS (Surveillance Camera System) or System applies to the University Surveillance Camera System including CCTV, Body Worn Video (BWV) and covert means.

3.2. The phrase SIA refers to the Security Industry Authority. The SIA are a government organization that are responsible for providing training and issuing licences to people who work in the security industry in the United Kingdom. The SIA Public Space Surveillance Licence is required by persons who are contracted to operate CCTV equipment in a public environment. Although these licences are not required for University of Surrey staff as they are directly employed by the University of Surrey, all operators will be provided with training to obtain this licence to ensure best practice.

3.3. In this Procedure, the phrases: "disclosure of data" and "release of data" could include a viewing of personal data and/or production of a copy of the personal data. The presumption under which this Procedure operates is that the viewing of data is sufficient for most circumstances. The release of a copy of personal data may only be authorized by the University Data Protection Officer or Legal Counsel or their agreed designate.

3.4. All footage that is recorded by the SCS is stored for 30 days. After this time it is automatically

overwritten. There are times when footage needs to be downloaded and stored as evidence for the police, staff disciplinary matters or student disciplinary matters. Footage for the police is kept for six months before it is deleted, footage for staff disciplinary matters is kept for seven years and footage for student discipline is kept for three years. This information is referred to as the retention schedule.

3.5. A Digital Evidence Management System (DEMS) is used to store video and audio footage from Body Worn Video (BWV). BWV is worn by all Security Officers as part of their uniform. DEMS is also used to store any covert recordings.

4. Procedural Principles

4.1 The cameras constituting the University CCTV system are actively monitored in the University's Control Rooms on Stag Hill campus and Manor Park campus. Remote monitoring of cameras is carried out at the Library and at Surrey Sports Park (SSP). University of Surrey (UoS) Library staff are able to view the cameras that are inside the library to assist with library usage and the monitoring of space as well as the safety of lone library users particularly out of hours. Library staff have no playback function available to them and they cannot download or save footage. Surrey Sports Park Duty Managers use the SCS to monitor usage of the playing fields and sports studios. This is to detect misuse and to assist in health and safety of lone people using the facilities. SSP Duty Managers are able to control SSP cameras but cannot playback or download recorded footage. SSP and Library Managers contact the Security Control Room for any footage that they wish to review, be saved or have downloaded.

4.2 Covert cameras will be deployed where appropriate and images secured via DEMS. Covert recording will only be used in exceptional circumstances where there is evidence of crime and when all other conventional and overt methods have been exhausted. The deployment of any covert devices will be used for the shortest time possible to reduce the possibility of collateral intrusion against those people whom the activity is not focused. This activity will be authorised by the Head of Security before any covert monitoring takes place. There will be regular reviews during any covert monitoring to ensure that it remains, proportionate, necessary and that it is meeting the aims of the authorisation. This monitoring will cease as soon as the outcomes have been achieved or it is found that the monitoring is not effective. While the University is not a Relevant Authority within the Regulation of Investigatory Powers Act 2000 and therefore not required to comply with the conditions of the Act, the guidelines of the Act will be followed to ensure best practice and full accountability.

4.3 Any request for recorded footage from CCTV or BWV will be entered onto a security incident report whether the requester is internal or external to allow for a clear audit trail. The name of the requester, the details of the footage they want and their justification for needing the footage will all be recorded. Request forms received from law enforcement agencies and other third parties will be sent to the Information Compliance Unit for approval. If approved, the data will be released and an update added to the incident report. If the request is refused, the reasons for refusal will be added to the incident report and the requester will be notified.

4.4 **Security Support Manager**

The Security Support Manager will:

- Ensure that this Procedure is adhered to
- Ensure that the functions of the Surveillance Camera System are implemented
- Ensure that Operators are supervised and developed and that they obtain a SIA Public Space Surveillance Licence
- Ensure that the interests of the University are upheld in accordance with the terms of this

Procedure

- Ensure that all faults relating to the system and any associated equipment forming part of the CCTV system are reported and adequately maintained and developed
- Consider reports from the Operators detailing the state of readiness of the equipment and the day to day and long-term operation of the system
- Liaise with relevant staff to ensure that the SCS Procedure remains compliant with legislation
- Facilitate viewing requests, including making arrangements to copy footage for potential viewings
- Ensure that Operators and other relevant staff are regularly reminded about the contents of this Procedure and any updates
- Ensure destruction of images in accordance with the retention schedule that is in place
- Monitor and supervise the daily procedural instructions, security of data and confidentiality.
- Ensure that at all times Operators of the SCS carry out their duties in an effective, efficient and responsible manner. This will include monthly checks of duty sign in logs, the retention of footage as well as checking records of how and when footage has been passed to third parties such as the police.
- A check of incident reports will be carried out monthly to ensure that the retention and storage of footage has been added to the reports where applicable.

4.5 **Control Room Operators**

Control Room Operators are responsible for taking appropriate action to deal with incidents detected through use of the system, and for keeping records as required by this procedure. Operators must:

- Carry out their duties in accordance with this Procedure and managerial instructions
- Control and operate the cameras and equipment forming part of the system with proficiency
- Ensure that information recorded by the system is accurate, adequate and relevant
- Justify decisions to view or record any particular individual, group or individuals or property
- Regularly refresh their knowledge of the contents of this SCS Procedure and CCTV manual

4.6 **Security Officers**

- At the commencement of each shift, all uniformed Security Officers will book out a Body Worn Video device via an authorised PC which has DEMS. There is one PC on Stag Hill campus and one at Manor Park campus that provides this function. This book out process will automatically record the user and attribute all recorded images to that user.
- On attending an incident whereby BWV images are considered to assist a disciplinary or criminal enquiry or otherwise be necessary for the purposes of safety and security, officers will activate the camera and then inform everyone present of the video and audio recording. The camera will be deactivated by the officer once the collection of relevant data is complete.
- On completion of their shift or when it is deemed necessary, an officer will connect the BWV device to a PC running DEMS to download the recorded footage. This will automatically book the device back in and provide a clear audit trail.
- Security Team Leaders and Deputy Team Leaders will have access rights to mark recorded images as evidential if it is likely to be required in any disciplinary hearing or if it is required by the police.
- The retention of footage captured by BWV is held in line with the wider SCS Procedure retention schedule detailed in section 3.4.

4.7 **Discipline:**

- Staff who impede the implementation of the SCS Procedure may be subject to disciplinary proceedings
- Breaches of the SCS Procedure or any aspect of confidentiality by staff with specific responsibilities under the terms of the SCS Procedure may be subject to the University's Staff Disciplinary Procedure
- Any unauthorised use or abandonment of the control room, it's systems and/or equipment for any purpose whatsoever apart from evacuation in an emergency) may amount to gross misconduct under the University Staff Disciplinary Procedure.

5. Governance Requirements

5.1. Implementation: Communication Plan

5.1.1. Security staff who access and monitor the SCS will be sent a link to this Procedure to ensure they have continual access to the most up to date copy.

5.1.2. This procedure will be published on the University's website to ensure transparency in the use of the SCS.

5.2. Implementation: Training Plan

5.2.1. All Control Room Operators will undertake training to obtain an SIA Public Space Surveillance Licence. This training will be provided by an external, accredited provider.

5.2.2. New staff will be given an induction to the SCS by the Security Support Manager and will be sent a link to this procedure so they can access the most up to date version.

5.3. Review

5.3.1. This Procedure will be reviewed every three years. Minor changes such as change of a role title or other titles or name which do not change the meaning of the Procedure will be made by the Authorised Owner, namely the Security Support Manager. Major changes will be anything that alters the meaning of this Procedure or are substantial. Re-writes are to be submitted via the full approval route.

5.4. Legislative Context and Higher Education Sector Guidance or Requirements

5.4.1. The University of Surrey is the Controller of the system and the owner of the data generated by the system.

5.4.2. Breach of this Procedure may result in disciplinary action being taken in accordance with the University's Staff Disciplinary Procedure.

5.4.3. The University recognizes that operation of the University Surveillance Camera System may be considered an infringement on privacy. The University acknowledges its obligations under the Human Rights Act 1998. The University also recognizes its obligation to provide a safe environment for staff, students and visitors and regards the use of SCS within the University as a necessary, proportionate and suitable tool.

5.4.4. The operation of the Surveillance Camera System has been registered with the Information Commissioner's Office in accordance with current UK Data Protection legislation. The registration number is Z6346945.

5.4.5. This policy adheres to the Our Data Policy, the Information Commissioner's SCS Code of Practice and the following legislation:

- Criminal Procedures and Investigations Act 1996
- Human Rights Act 1998
- Data Protection Act 2018 (incorporating the UK General Data Protection Regulation)
- Crime and Disorder Act 1998
- Equalities Act 2010

5.4.6. All personal data will be processed in accordance with the Principles of the UK General Data Protection Regulation.

- All personal data will be processed fairly, lawfully and in a transparent manner
- Personal data will only be processed for specified, explicit and legitimate purposes
- Personal data will be adequate, relevant and limited to what is necessary
- Personal data will be accurate and where necessary, kept up to date
- Personal data will be held no longer than necessary
- Procedures are in place to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.

5.5. **Sustainability**

5.5.1. The use of a SCS requires electrical power. The system runs 24/7 and is required to do so in order to capture best evidence and to help maintain the health and safety of staff, students and visitors as well as to prevent and detect crime.

5.5.2. To stop unnecessary wastage, there will be no paper copies of this Procedure unless requested.

6. Stakeholder Engagement and Equality Impact Assessment

6.1. An Equality Impact Assessment was completed on 13/02/2023 and is held by the Authorised Co-ordinator.

6.2. Stakeholder Consultation was completed, as follows:

Stakeholder	**Nature of Engagement**	**Date**	**Name of Contact**
Information Governance	Review by the DPO of this Procedure	06/04/2023	Ewan Robson
H&S	Review by Health & Safety	20/02/2023	Paul Daniell
Governance	Review by Governance	16/02/2023	Andrea Langley
Sustainability	Review by Sustainability	20/03/2023	Martin Wiles
Chair of the Compliance sub-committee, University Secretary and General Counsel (USGC)	Review by University Secretary and General Counsel	18/04/2023	Sarah Litchfield