Surveillance Camera System Policy	
Operational Owner:	Deputy Head of Security
Executive Owner:	Director of Estates & Facilities Management
Effective date:	October 2019
Review date:	October 2022
Related documents:	Information Security Policy Surveillance Camera Systems Procedure

Approval History

Version	Reviewed by	Approved by	Date
1	Legislative and/or key stakeholder sign off	M Hassell/ C Parkinson	29 May 19/ 20 Feb 19
1.1	Owner sign off if different from author	Stephen Wells	8 Aug 19
1.1	Data and Information Security Steering Committee	Approved with amendments	8 Oct 19
2	Executive Board sign off		24 Oct 19

1	**Introduction**
1.1	**Purpose**
1.1.1	The University of Surrey believes that Surveillance Camera Systems (SCS) incorporating CCTV, BWV (Body Worn Video) and covert means of recording images and audio are a powerful tool to assist with efforts to enhance community safety, and that the operation of SCS should be controlled to avoid the potential of misuse. The Information Commissioner's SCS Policy provides a framework for the operation of SCS. The University supports this Policy, which is applied in the context of the University of Surrey through this SCS Policy & Procedure.
1.2	**Scope**
1.2.1	All staff and students of the University are subject to the SCS Policy and are required to contribute, on request, to the application of this Policy.
1.2.2	Staff who have been designated as having responsibility for the management and the operation of the Surveillance Camera Systems are required to undertake their responsibilities strictly in accordance with this Policy, and the associated Procedure. Such staff are required to operate the Surveillance Camera Systems fairly, within the law, and only for the objectives identified in this Policy.

1.3	**Definitions**
1.3.1	Any reference in this document to 'CCTV', 'SCS System', 'SCS' or 'System' applies to the University Surveillance Camera Systems (CCTV, Body Worn Video (BWV) and covert means). The cameras constituting the University CCTV System are actively monitored in the University's control room. Remote monitoring of cameras at Surrey Sports Park and the Library are monitored but not controlled by staff at those locations. BWV is worn and operated by uniformed Security Officers Covert images will be managed through Digital Evidence Management Solution (DEMS)
1.3.2	In addition to the permanently fitted cameras the University also deploys Body Worn Video (BWV) through its patrolling Security Officers which captures audio and video data and images secured through a Digital Evidence Management Solution (DEMS) application. Covert camera images will be deployed where appropriate and images secured via DEMS.
1.3.2	In this Policy, the phrases "disclosure of data", and "release of data" could incorporate a viewing of personal data and/or production of a copy of the personal data. The presumption under which this Policy operates is that the viewing of data is sufficient for most circumstances. The release of a copy of personal data may only be authorised by the University Data Protection Officer or Legal Counsel or their designate.
2	**Policy**
2.1	**Objectives**
2.1.1	This Policy aims to ensure that SCS on University of Surrey premises are operated to enhance safety, and the sense of safety; and thereby assist in encouraging use of University facilities, through the following subsidiary objectives: 1. To assist in deterring crime 2. To assist in detecting crime and to provide evidential material for court proceedings 3. To assist in the overall management of buildings and land within the boundaries of the University 4. To assist in monitoring, and planning for, emergency operations; and to assist the Police, Fire, Ambulance and Civil Emergency Services with the efficient deployment of their resources to deal with emergencies. 5. To assist in the investigation of Health & Safety incidents.
2.1.2	This Policy aims to ensure that SCSs are used transparently and proportionately to achieve the objectives identified in Section 2.1, in compliance with the law and the Information Commissioner's SCS Code of Practice.
2.1.3	The reference in 2.1.1 (3) to "the overall management of buildings and land" incorporates but is not limited to such matters as monitoring of traffic flow, car-park capacity, defects in bollard operation, defects in lighting, and damage to buildings.
2.2	**Core Obligations**
2.2.1	The University will identify the locations of all cameras connected to the University's SCS System and will monitor, and manage, images shown on these cameras in accordance with this Policy and the associated Procedure.
2.3	**Data processing**

2.3.1	CCTV and BWV images are recorded 24/7 and are held in central data storage. In each case images are retained for 28 days as a default before being deleted. Other retention periods are subject to schedules: Required at Student Disciplinary Panel 2 years Required at Staff Disciplinary Panel 7 years Required for Police use 6 months
2.3.2	All requests for new cameras will be subject to a review by the Deputy Head of Security to ensure necessity and conformity with the stated purpose.
2.3.3	Body Worn Video will be deployed subject to procedure and commence with a warning to data subjects that BWV has been deployed and is recording audio and video.
2.3.4	Covert devices will only be deployed on the direction of the Head of Security or in his/ her absence, the Deputy Director of Estates following a review of attempts to capture evidence by less intrusive methods. The application and deployment process will apply due consideration to the principles of the Regulation of Investigatory Powers Act 2000 and will be detailed in the accompanying Procedures. Ratification of each application and authorisation will be provided by the University Data Protection Officer.
2.4	**Data Recorded**
2.4.1	Data recorded could include: • People – including facial images and activities • Vehicles – including registration plates and movement • Audio – where body worn video or covert devices are deployed.
2.5	**Human Rights**
2.5.1	The CCTV system, BWV and covert devices will only be used as a proportional response to identified problems and may only be used insofar as is necessary, in the interests of national security, public safety, the prevention and detection of crime or disorder, the protection of health, the protection of the rights and freedoms of others, the management of buildings and land, and assistance in the resolution of a factual disagreement which emerges during investigation of a grievance, complaint or disciplinary allegation. A proportional response will be determined by reference to the purpose deployment is intended against the rights of data subjects whose activities will likely be recorded.
2.5.2	The University Surveillance Camera Systems shall be operated with respect for all individuals, recognising the right to private life (ECHR Article 8). It shall also recognise the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, ethnicity, disability, sexuality, language, religion, political or other opinion, property, birth or other status.
2.6	**Release of Personal Data, Following a Personal Request for Information**
2.6.1	Any request from an individual for the disclosure of personal data under the General Data Protection Regulation or other Data Protection Legislation, or for disclosure under the Freedom of Information Act, which he/she believes is recorded by virtue of the system, should be made, in the first instance, to the Information Compliance Unit.

2.6.2	Articles 12-22 of the General Data Protection Regulations (relating to the rights of data subjects) shall be followed in respect of every request.
2.6.3	Any person making a request must be able to prove his/her identity and provide sufficient information to enable the data to be located.
2.6.4	The University Data Protection Officer or Legal Counsel are authorised to view SCS images in order to process a Subject Access Request.
2.6.5	If a request can only be complied with by identifying another individual, or several individuals, arrangements must be made to safeguard the rights of that individual or individuals, such as obtaining permission from that individual or individuals or blocking of the image of that individual or individuals.
2.6.6	Where the University Data Protection Officer or Legal Counsel authorises a viewing of a SCS image by the individual whose personal data is recorded on the image, that individual may be accompanied during the viewing by a friend or by a representative from the individual's Trade Union.
2.6.7	Authorised viewings of personal data will normally take place in the Security Manager's Office.
2.7	**Release of Personal Data as Required by Law**
2.7.1	As required by law, the Deputy Head of Security may authorise Security Personnel to release personal data to members of the police service, or other agency having statutory authority to investigate and/or prosecute offenders.
2.7.2	Each and every application will be assessed on its own merits and 'blanket exemptions' will not be applied. In order that the University can show 'due diligence' in determining whether such information should be released, a Data Request form will be completed by the applicant (including the police) following which the Security recipient will determine whether such data requested should be released.
2.7.3	Members of the police service, or other agency having a statutory authority to investigate and/or prosecute offenders, may release to the media details recorded by the University, only in an effort to identify alleged offenders, or potential witnesses, and only in accordance with their responsibilities as the new Controller of the data.
2.8	**Release of Personal Data to a Person who is not the Data Subject**
2.8.1	A University Senior Manager* who is investigating a complaint, grievance, or disciplinary allegation, under a formal University process; or who is investigating a Health & Safety incident must seek authorisation from the University Data Protection Officer or Legal Counsel for release of the personal data contained in an image which has been obtained during surveillance of the campus, in accordance with the objectives stated in Section 2 of this Policy.
2.8.2	The University Data Protection Officer or Legal Counsel may grant such authority, in writing, where he/she is satisfied, <u>either</u>: a) that there is prima facie evidence of an allegation which exists independently of the image, and prior to the request for authorisation <u>or</u> b) that an incident occurred affecting the Health and Safety of any person, <u>or</u> c) that the allegation relates to criminal activity <u>or</u>

	d) that both parties have agreed that it would be beneficial for the University Senior Manager to view the image, or e) that one (or more) party has already viewed the image (having submitted an application to view on the grounds of being recorded in the image).
2.8.3	* *(For the purposes of this Policy, a "University Senior Manager" is a School Manager, an Assistant Dean, an Assistant Director or a person of more senior status.)*
2.9	**Complaints**
2.9.1	Any student, member of staff or the general public wishing to register a complaint with regard to any aspect of the system may do so by contacting the Deputy Head of Security in the first instance. Data Protection concerns may be referred to the Information Compliance Unit.
2.10	**Copyright**
2.10.1	The University of Surrey retains ownership of copyright and of all material recorded by the systems.
3	**Governance Requirements**
3.1	**Implementation / Communication Plan**
3.1.1	This Policy will be published on the University's web site together with updated templates and all University Policy Documents (either direct or clearly linked to other pages).
3.2	**Exceptions to this Policy**
3.2.1	The only exception to this policy is the use of web based cameras, which do not record and which are for use in the provision and maintenance of services such as AVS in lecture theatres.
3.3	**Review and Change Requests**
3.3.1	This policy will be reviewed every 3 years. Minor changes such as change of a role title or other titles or name which do not change the meaning of the policy will be made by the operational owner. Major changes will be anything that alters the meaning of the policy or are substantial re- writes are to be submitted via the full approval route.
3.4	**Legislative context**
3.4.1	The University of Surrey is the "data controller "of the system and the "owner" of the data generated by the system.
3.4.2	Overall responsibility for the implementation of the Policy has been delegated by the Vice-Chancellor to the Head of Security or their designate.
3.4.3	Breach of this Policy and the associated Procedure may result in disciplinary action being taken in accordance with the University's Staff Disciplinary Policy and Procedure.
3.4.4	The University recognises that operation of the University Surveillance Camera Systems may be considered an infringement on privacy. The University acknowledges its obligations under the Human Rights Act 1998. The University also recognises 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.

3.4.5	The operation of the system has been registered with the Information Commissioner's Office in accordance with current Data Protection legislation.
3.4.6	This Policy and the SCS Procedure take account of the University's Data Protection 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 General Data Protection Regulation) • Crime and Disorder Act 1998 • Equalities Act 2010
3.4.7	All personal data will be processed in accordance with the Principles of the General Data Protection Regulation which include, but are not limited to: i. All personal data will be processed fairly and lawfully (The definition of 'processing' covers 'obtaining') ii. Personal data will only be processed for the purpose specified iii. Personal data will be adequate, relevant and not excessive iv. Personal data will be accurate and where necessary kept up to date v. Personal data will be held no longer than necessary vi. Individuals will be allowed access to information held about them and, where appropriate, will be permitted to correct or erase it vii. Procedures will be implemented to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.
3.5	**Stakeholder Statements**
3.5.1	Equality: The University is strongly committed to equality of opportunity and the promotion of diversity for the benefit of all members of the University community. The University's approach is to promote equality across the full range of its activities, in employment, teaching and learning and as a partner working with and within local, national and international communities. Equality Analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact on equality has been identified.
3.5.2	Health & Safety: Health and Safety implications have been considered during the drafting of this policy and are incorporated (where necessary) into the policy.