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.

Surveillance Camera System (SCS) Procedure

This Procedure accompanies the University's Surveillance Camera System Policy which regulates the operation of University of Surrey's Surveillance Camera Systems. The purpose of the SCS Procedure is to support the objectives of the Policy by outlining how the University will implement the SCS Policy.

Extract from the University of Surrey SCS Policy

This Policy aims to ensure that SCS on University of Surrey premises is 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.

CONTENTS

1. General Principles

1.1 Lawful – The system will be operated in accordance with the law, including, in particular, the Data Protection Act 2018 which incorporates the General Data Protection Regulation, and the Human Rights Act 1998. The Surveillance Camera Systems may not be used where the privacy of individuals would clearly be violated, provided a criminal offence is not taking place.

1.2 Restricted Application – The system shall be operated fairly, within the law, and only for the purposes stated in the SCS Policy. Any individual or authority/organisation utilising the Surveillance Camera Systems must comply fully with this Procedure and will be held accountable under the SCS Policy and this Procedure.

1.3 Balanced – The University will balance the public interest in achievement of the objectives of the Surveillance Camera Systems and the public interest in the operation of the systems, including the security, transparency and integrity of all operational procedures in relation to SCS. Consequently, a formal structure has been put in place, including a complaints procedure, by which it can be demonstrated that the systems are accountable, and are also seen to be accountable.

2. Cameras and Coverage

2.1 The areas covered by the University's Surveillance Camera Systems, to which this Procedure refers, include public areas and areas within the responsibility and/or perimeter boundaries of the University of Surrey, including within University buildings.

2.2 Signs will be placed at the main entrance points to the University to indicate:

- The presence of CCTV
- The purpose of the CCTV
- Ownership of the CCTV system
- Contact details

Signage will also be placed at entrances to the buildings where internal CCTV cameras are in operation.

2.3 Some cameras may be enclosed within all-weather domes for aesthetic or operational reasons, but the presence of cameras connected to the University's CCTV system will be identified by appropriate signs.

2.4 Body Worn Video cameras worn and operated by uniformed Security Officers will record audio and video. Use of equipment will be in accordance with Security Standard Operating Procedure 005.

2.5 Covert devices will only be deployed after consideration of the circumstances in which deployment has been considered. The application and deployment process will apply due consideration to the principles of the Regulation of Investigatory Powers Act 2000, and the person making the application will provide details of all other means to secure evidence to the Head of Security or in his/ her absence, the Deputy Director of Estates. Application and authorisation or other direction will be by email.

3. Monitoring and Recording Facilities

3.1 The central Security Control Room (referred to as "the control room"), is staffed by Security CCTV operators.

3.2 University CCTV operators are able to replay images, and produce hard copies of recorded images, in accordance with this Procedure and associated Policy. Viewing and recording equipment may only be operated by trained and authorised operators.

3.3 The Security Manager may view all cameras from his/her Office.

3.4 In certain circumstances, University staff other than the CCTV operators may be granted viewing rights (live images only) for one or more cameras on the CCTV system. This includes staff at the Library and Surrey Sports Park.

3.5 Images recorded on BWV will be downloaded into DEMS (Digital Evidence Management Solution) and access restricted by password and role sensitive rights. DEMS is only available on a limited number of identified PCs.

4. Operation of the CCTV System

4.1 All persons operating CCTV cameras must act with the utmost probity at all times. Operators are required to sign a declaration of confidentiality (Annex A).

4.2 The Deputy Head of Security is required to provide all individuals operating the CCTV system with a copy of the SCS Policy and Procedure. All relevant staff are required to sign to confirm that they fully understand their obligations as set out in the SCS Policy and Procedure.

4.3 A Manual containing technical instructions on the use of the equipment will be housed in the control room electronic folder (Teams).

4.4 The control room and monitoring system must be staffed, at all times, by at least one Officer. Any unauthorised use or abandonment of the University control room and its systems and equipment for any purpose whatsoever (apart from evacuation in an emergency) may amount to gross misconduct under the University's Staff Disciplinary Procedure. If the control room must be vacated in an emergency, for safety or security reasons, the Manual must be followed (Annex C).

4.5 Only members of staff authorised by the University to operate the CCTV system may have access to the operating controls. Those operators will have primacy of control at all times.

5. Maintenance of the CCTV System

5.1 To ensure compliance with the Information Commissioner's Code of Practice, and to ensure that images recorded continue to be of appropriate evidential quality, the system shall be maintained in accordance with the requirements of the procedural manual under a maintenance agreement. User requirements can be maintained by a member of Security Personnel. Faults will need to be maintained by a CCTV Engineer.

5.2 The maintenance agreement will make provision for:

- Regular service checks on the equipment, including cleaning of any all-weather domes or housings, checks on the functioning of the equipment and any minor adjustments that need to be made to the equipment to maintain picture quality.

- Regular overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.
- "Emergency" attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

5.3 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem, depending upon the severity of the event and the operational requirements of the system.

5.4 Appropriate records of faults must be maintained by the Deputy Head of Security in respect of the functioning of the cameras/system and the response of the maintenance organisation. (Annex B-1)

6. Access to, and Security of, Control Room and Associated Equipment

6.1 Only authorised operators who have been certified as appropriately instructed may operate any of the equipment located within the control room. A list of all authorised operators will be maintained in the control room by the Deputy Head of Security. An authorised operator must be present at all times when the equipment is in use.

6.2 The following are authorised to visit the control room:

The Head and Deputy Head of University Security Services
CCTV/ Alarm engineers
University cleaning staff
Estates "on-call staff"
Police in the pursuance of their duties

The names of visitors must be recorded, and visitors must be accompanied at all times by an authorised operator or the Deputy Head of Security.

6.3 Public access to the control room will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the Deputy Head of Security. Any such visits will be conducted and recorded in accordance with this Procedure.

6.4 Regardless of their status, all visitors to the control room will be required to read the declaration of confidentiality prior to signing the visitors' book. (Annex C-2). Refused visitor details will also be recorded in the visitors' book. Duty controllers must be satisfied that visitors can be accurately identified and that the purpose of their visit is valid.

7. Management of Recorded Material

7.1 For the purposes of this Procedure, "recorded material" means any material recorded by, or as a result of, the technical equipment which forms part of the Surveillance Camera Systems, but specifically includes images recorded digitally, or by way of video copying, inclusive of video prints. Every recording obtained using the system has the potential of containing material that may be admitted as evidence in a Court of Law at some point during its life span.

7.2 It is of the utmost importance that, irrespective of the format of the images obtained from the system, recorded material is treated strictly in accordance with this Procedure from initial recording to date of destruction. All movement and usage of material must be recorded (Annexes B-3, B-4, B-5, B-7).

7.3 Access to, and the use of, recorded material must be strictly in pursuance of the purposes defined in the University's SCS Policy.

7.4 Recorded material may not be copied, sold or otherwise released or used for commercial purposes, personal use, or for the provision of entertainment.

7.5 All material recorded by the system will be retained for 21 days before being overwritten or erased. Recordings may only be retained beyond this period in the following circumstances:

- Where evidential material exists which is likely to be required by the Police. (This should be kept for duplication and subsequent production in Court.)
- Where material is required following a Subject Access Request submitted within 14 days of the incident.
- Where material is required as part of a Freedom of Information Request
- Where the evidence is required under a Court Order.
- Where the Vice-Chancellor, or the University Secretary, informs the Security Manager that the maintenance of the material is in the interests of the University, and in accordance with the SCS Policy.

In these circumstances, the CCTV material will be copied to the control room CCTV PC and copied to disc as required in accordance with this Procedure.

7.6 To ensure the quality of recorded material, only new, one-time recordable discs may be used. Each disc will be marked with the University of Surrey Incident number and an exhibit reference number utilising the Operator's initials.

7.7 The destruction of discs is to be recorded in the Data Destruction Register. (Annex B-6)

7.8 Images from every camera will be recorded continuously throughout a 24-hour period.

7.9 All recorded images will be identified by camera number, date recorded and time group. Images may only be reviewed by University Security Officers, Security Managers, or by such other persons as are authorised by this Policy/Procedure**.** (Annex B-7)

7.10 Media prints will not be taken as a matter of routine. Justification must be provided for each print. Details of all media prints will be recorded (see Annex C-3)

7.11 In the event of any recorded material being required for evidential purposes, the processes outlined in the Procedure and manual must be strictly complied with.

7.12 Images recorded in DEMS will be subject to the same documentation and processes as CCTV images when data is requested, viewed or provided.

7.13 all correspondence relating to requests, authorisations and reviews of covert surveillance measures will be provided to the Data Protection Officer who will retain them for 5 years before being weeded and destroyed.

8. Request for Information/Release of Data

8.1 Members of the University community and general public who believe their image has been captured by the system have the right to view relevant footage at a time convenient to themselves and to the University. To this end, an individual, and/or his/her legal representative, may request a viewing or a copy of the footage by writing to the University's

Data Compliance Officer. Directions regarding Subject Access Requests can be found at https://www.surrey.ac.uk/information-management/data-protection .

8.2 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.

8.3 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must only be shown after prior approval for disclosure is granted by the Head of Legal Counsel (Legal Services) or person of equivalent status.

9. Responsibilities

9.1 Deputy Head of Security

The Deputy Head of Security will:

- Ensure that the Policy and Procedure are adhered to.
- Ensure that the functions of the CCTV system are implemented.
- Ensure that operators are supervised and developed.
- Ensure that the interests of the University are upheld in accordance with the terms of the Policy and 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.
- In consultation with the operators and other relevant individuals, investigate and propose alterations, additions or amendments to the system.
- Liaise with relevant staff to ensure that SCS Policy and 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 the Policy and Procedure, and any updates.
- Ensure destruction of images, in accordance with protocols.
- Monitor and supervise the daily procedural instructions, security of data and confidentiality.
- Ensure that at all times operators of the SCSs carry out their duties in an efficient and responsible manner. This will include regular checks and audit trails to ensure that any documentation is relevant and up to date.

9.2 Operators

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 Handbook.

Operators must:

- Carry out their duties in accordance with the Policy, the 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, relevant and does not exceed that necessary to fulfil the purpose of the system.
- Justify decisions to view or record any particular individual, group of individuals or property, when requested by the supervisor or manager.
- Regularly refresh their knowledge of the contents of the SCS Policy and Procedure, and manuals.

10. Discipline

10.1 Staff or students who impede implementation of the SCS Policy may be subject to disciplinary proceedings.

10.2 Breach of the SCS Policy, Procedure or any aspect of confidentiality by individuals with specific responsibilities under the terms of the SCS Policy and Procedure may be subject to University's Staff Disciplinary Policy.

10.3 Any unauthorised use or abandonment of the control room, its 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.

11. Complaints

11.1 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 Head of Security Services in the first instance. Data Protection concerns may be referred to the Information Compliance Unit Manager.

11.2 Should the matter remain unresolved, a formal complaint may be submitted to the Director of Estates, Facilities & Commercial Services. The issue may be investigated under the Student Complaint Procedure, the Staff Grievance Procedure, or the special procedure for consideration of data protection matters, culminating in an appeal to the DPA/FOI Complaints Panel.

12. Annexures

Annex A – Declaration of Confidentiality
Annex B – Relevant Documentation
Annex C –Control Room Evacuation Guidelines

Annex A

Declaration of Confidentiality

University of Surrey SCS System

I, (…….. D.O.B ……..) am employed by the University of Surrey in the capacity of ……. to perform the duty of SCS Control Room Operator /Supervisor/Manager. I have received a copy of the SCS Procedural Manual in respect of the operation and management of that SCS System.

I hereby declare that:

I am fully conversant with the content of that SCS Procedural Manual and understand that all duties which I undertake in connection with my employment must not contravene any part of the current Procedural Manual, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the system or the content of the Code of Practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation any information which I may have acquired in the course of, or for the purposes of, my position within the SCS control Room. I also understand this undertaking will apply for a period of one year after the cessation of my employment in connection with the SCS control room.

In appending my signature to this declaration, I agree to abide by the Procedure Manual at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format - now or in the future.

Signed: .....

Print Name: .....

Witnessed: ..... Position: .....

Dated the ..... day of .....

Maintenance Log – External SCS Cameras

Camera	Name		
Camera Type		Camera Location	

Date of Fault	Description	Estates Ref	Date of Repair	Remarks

Control Room SCS Equipment – General

Date of Fault	Description	Estates Ref	Date of Repair	Remarks

Maintenance Log – Control Room Recording Equipment

Equipment		**Function**	
Serial Number			
Date of Fault	**Description**	**Estates Ref**	**Date of Repair**

WARNING

RESTRICTED ACCESS AREA

Everyone, regardless of status, entering this area is required to complete an entry in the Visitors book.

Visitors are advised to note the following confidentiality clause and to understand that entry is conditional on acceptance of that clause.

CONFIDENTIALITY CLAUSE

'In being permitted entry to this area you acknowledge that you agree not to divulge any information obtained, overheard or overseen during your visit. An entry, accompanied by your signature in the Visitors' book is your acceptance of these terms'

University of Surrey SCS System

(Visitors Log Control Room)

Note: **In signing this visitors book all visitors to the University of Surrey SCS Control Room acknowledge that personal details of those operating the system, is, and should remain confidential.**
You further agree not to divulge any information obtained, overheard or overseen during your visit.

Date	Name	Company/Dept	Signature	Reason	Time In	Time Out

Serial No:

UNIVERSITY of SURREY SECURITY MEDIA PRINT REGISTER

Security Incident No		Date Produced	
Reason for Production			
Operator Name		Issued To (Name)	
Operator Signature		Signature	
Date		Date	

Security Incident No		Date Produced	
Reason for Production			
Operator Name		Issued To (Name)	
Operator Signature		Signature	
Date		Date	

Security Incident No		Date Produced	
Reason for Production			
Operator Name		Issued To (Name)	
Operator Signature		Signature	
Date		Date	

Security Incident No		Date Produced	
Reason for Production			
Operator Name		Issued To (Name)	
Operator Signature		Signature	
Date		Date	

Note: Data Destruction Register is to be completed when printed media is returned to Security and no longer required for evidential purposes.

Annex B-5

DIGITAL SCS EVIDENCE REGISTER Sheet Ser No_____

MASTER	Serial No	
COPY	Serial No	

DVD PRODUCTION	
Date Produced	
Produced By	
Signature	

ISSUE DETAILS			
Issued By		Issued To	
Date		Date	
Signature		Signature	

Both Master & Working Copies to be Issued.

RECORDING DETAILS			
Recorder Location			
Camera No(s)		Date & Time of Incident	
Incident No/Reference			
Brief Details			

Notes:

- Data Destruction Register is to be completed when the DVD's are returned to Security and no longer required for evidential purposes.
- All DVDs that fail to record should be recorded in the Data Destruction Register and then destroyed
- **No DVD is to leave the Control room unless it is signed for.**

DATA DESTRUCTION REGISTER

DESTRUCTION NOTES

1. **DVD/CD**

a Data Destruction Register is to be completed when the DVDs are returned to Security and no longer required for evidential purposes.

b Details of all DVDs that fail to record, are to be recorded in the Data Destruction Register and then destroyed .

c No DVD is to leave the Control Room unless it is signed for.

d Score the disk with an abrasive; the disk should then be snapped/bent in half to prevent use.

2. PRINTED MEDIA

a Data Destruction Register is to be completed when printed media (Images) are returned to Security and no longer required for evidential purposes.

b Details of all Still Images that are not required or are poor quality, are to be recorded in the Data Destruction Register and then destroyed.

c No Image is to leave the Control room unless it is signed for.

d All printed media (still images/reports etc) are to be destroyed by shredding.

Annex B-6

Sheet No…….

DATA DESTRUCTION REGISTER				
Ser	Date	Data Type/Serial No	Destroyed By	Signature

Serial No

UNIVERSITY of SURREY SECURITY - VIEWING LOG - RECORDED MEDIA

System	**CCTV**				
Building (Internal Only)					
Camera Number(s)					
Reason for Viewing					
Outcome of Viewing					
Date		Viewed By		Signature	
Still Image(s) Produced	YES / NO	(If YES see Media Print Register for details)			

System	**CCTV**				
Building (Internal Only)					
Camera Number(s)					
Reason for Viewing					
Outcome of Viewing					
Date		Viewed By		Signature	
Still Image(s) Produced	YES / NO	(If YES see Media Print Register for details)			

System	**CCTV**				
Building (Internal Only)					
Camera Number(s)					
Reason for Viewing					
Outcome of Viewing					
Date		Viewed By		Signature	
Still Image(s) Produced	YES / NO	(If YES see Media Print Register for details)			

Annex C

SECURITY CONTROL ROOM –EVACUATION PROCEDURE

In the event that the Security Control Room is to be evacuated in an emergency the following guidelines are to be followed by the Control Room Officer.

SHORT TERM EMERGENCY EVACUATION

1. Inform all radio call signs that you are evacuating the control room.
2. Collect the handheld radio and the Emergency Log Book. This will maintain radio communications and a written record of events.
3. If time allows, secure all windows.
4. If time allows, log off desktop PC and switch off all monitors.
5. Leave control room ensuring the access door is secured to prevent unauthorised access.

LONG TERM EVACUATION

1. Inform all radio call signs that you are evacuating the control room and moving to fall-back location, confirmed by Security Manager/Supervisor.
2. Transfer forward telephones to fall-back location.
3. Collect all available radios/chargers and the Emergency Log Book. This will maintain radio communications and a written record of events.
4. If time allows, secure all windows.
5. If time allows, log off desktop PC and switch off all monitors.
6. Leave control room ensuring the access door is secured to prevent unauthorised access.

In the event access is required to the Control Room by the Emergency Services, they should be accompanied by a Security Officer unless the situation is deemed too dangerous. If that is the case then the Emergency Services should be allowed unaccompanied access.