



Title: CCTV Policy

Author: J.Hollow

Date:02.02.24


Doc No.: Admin /E&F /EandFDocumentManagement /
Facilities /Security /CCTV/ CCTVPolicy

Version: 4

Review Date: 02.02.26

CCTV Policy

Rev	Date	Amendment	Approved & Authorised by
1	16/09/11	Issued	J.Hollow/V.Williams
2	10/08/17	Changed of Titles, Removal of Sports Centre, Student Union & Horton Halls from lone monitoring. Change of Planning & Secretariat Department to Governance, Legal & Assurance Services	E Gilby
3	25/04/18	Change of Job Title	
4	02/02/24	Document overhaul	

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

CCTV Policy

Introduction

As in most other Universities CCTV is seen as one of the most effective physical security measures. The use of cameras enables greater security coverage within SGUL premises thereby increasing safety. SGUL has external and internal cameras designed to deter and detect crime and safeguard staff, students and visitors to the organisation.

St George's, University of London (SGUL) (the "University") is the owner of a public closed circuit television systems (CCTV) currently installed around the site and in the Halls of Residence. In addition, the system may incorporate body worn and covert cameras where required.

For the purpose of this policy these systems together will collectively be known as the CCTV system.

There are several types of camera –

- Overt fixed – these record uncontrolled images e.g. reception desk, doors etc.
- Overt Pan, Tilt, and Zoom (PTZ) – these are controllable cameras that can follow vehicles or subjects when required.
- Body worn – can be used by security staff when on late night patrols and dealing with drunkenness, violence, and anti-social behaviour.
- Covert cameras – temporary fitted cameras used in areas not covered by CCTV but the scene of persistent criminality.


CCTV monitoring and recording systems will only be installed in or on university property when this has been reviewed and approved by the Director of Estates and Facilities. Independently installed and operated CCTV systems by staff / students will not be permitted on any University property and where found actions will be taken to close these systems down.

Images are recorded locally within locations or centrally on servers held under SGUL Security control; they are generally all viewable centrally by security staff (Exceptions being DR Room, and internal cameras of F Block). In addition, a limited number of management staff may have the facility to monitor cameras sited within their own areas of responsibility.

This policy reflects the spirit and guidance issued by the Information Commissioner's Office as documented in the 'CCTV Code of Practice revised edition 2008' and will not be used to invade the privacy of any individual, residence, business or other private premises, buildings or land.

This policy should be read in conjunction with the SGUL Security Policy and the Information Commissioner's Office CCTV Code of Practice Revised Edition 2008.

All images produced by the system remain the property and copyright of SGUL.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

The following principles will govern the operation of the CCTV system.

1. The CCTV system will be operated fairly and lawfully and only for the objectives authorised by SGUL.
2. The CCTV system will be operated with due regard for privacy of the individual.
3. Any changes to the objectives will be publicised in advance.

Objectives for the use of CCTV systems

The objectives for the use of the various CCTV systems are to:-

- Assist in providing a safe and secure environment for the benefit of those who might visit, work, or live in the University.
- Reduce the fear of crime by reassuring students, staff and visitors.
- Deter and detect crime, public disorder, and anti-social behaviour.
- Identify, apprehend, and prosecute offenders in relation to crime, public disorder, and anti-social behaviour.
- Provide the Police, the Health and Safety Executive and the University with evidence upon which to take criminal, civil and disciplinary action respectively.
- Monitor and assist with traffic management.
- Assist in the monitoring and deployment of security staff during normal duties and emergency situations.
- Protect security officers, staff and students from undue threats and violence.
- Obtain evidence against persistent offenders stealing from staff, visitors, and students.

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than the situations covered under "Covert Recording"..
- For any automated decision making

Responsibilities


The Director of Estates and Facilities retains overall responsibility for the system and delegates the management of the system to the Facilities Manager- It is their responsibility to ensure that CCTV within the University is managed in line with this policy at all times.

For the avoidance of doubt all requests and permissions should be made to the Facilities Manager in the first instance. If they are not available then the Director of Estates and Facilities. No other individual can take this responsibility unless it has been specified in writing in advance from one of the two aforementioned individuals.

The Vice Chancellor is responsible for giving permission for the installation of covert recording devices and to review CCTV images (current or recorded) which will involve the monitoring of staff or students either overtly or covertly which could lead to action or investigation by Human Resources, Registry, IT or other SGUL departments.

It will be the responsibility of the Facilities Manager to:

- Select camera sites and initial areas to be viewed.
- Be responsible for compliance with the Data Protection Act (DPA).
- Take responsibility for control of the images and make decisions on how these can be used.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

- Oversee and ensure cancellation of any covert recording operation.
- Ensure the system is secured and only viewed by authorised persons.
- Ensure that the procedures of this Code of Practice comply with the current CCTV Codes of Practice produced by the Information Commissioner's Office.
- Make annual checks to establish that nominated individuals still require viewing rights of the system in line with the above objectives.
- Ensure that all Data Protection Act forms received from the Police or other investigatory bodies e.g. Health and Safety Executive are filed for future reference.
- Ensure adequate signage is erected.
- Regularly evaluate the system to ensure it complies with the latest legislation, CCTV Codes of Practice and its use is in accordance with these Codes of Practice.
- Clearly communicate the specific purposes of the recording of and use of images and objectives to all security staff.
- Ensure that a CCTV incident log and record of Police or other Statutory Authority requests for images is maintained.
- Carry out annual audits to check that procedures are being complied with.
- Ensure that regular 3 monthly reviews are conducted of all locked images and delete those not still required for evidential purposes.
- Ensure that all data and images are erased after a period of 3 months unless locked or retained for evidential purposes.

The Facilities Manager may delegate some of the responsibilities for day-to-day management of the system to the security manager.

It will be the responsibility of the individual Security Officer / Supervisor to:

- Select appropriate images to be recorded on controllable cameras (Pan-Tilt-Zoom PTZ) so as to comply with the objectives outlined above.
- Ensure that targeting of individuals with the cameras is only conducted when there is reasonable suspicion that the person falls within one of the objectives set above e.g. committing a criminal offence.
- Not to view into private property and be mindful of student privacy within student accommodation.
- Complete the CCTV incident log / VMS as appropriate.


Covert Recording

It is considered essential that occasionally it would be beneficial not just to deter but, in selected instances, to catch perpetrators of illegal activity so that more appropriate action can then be taken. Covert cameras will be used on rare occasions when a series of criminal acts have taken place e.g. thefts in the same area not fitted with CCTV.

Covert cameras may be used under the following circumstances on the written authorisation or request of the Vice Chancellor to ensure;

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

suspected unauthorised activity. Consideration will be given to any intrusion on innocent individuals.

Covert recording devices should not be installed in private areas such as toilets and private offices, except in the most exceptional circumstances where serious crime is suspected. This should only happen where there is an intention to involve the police, not where it is a purely internal disciplinary matter.

In some cases, covert cameras installed for one investigation may turn up evidence of other criminal behaviour or disciplinary offences. This should be acted upon where the offence is serious, for example, gross misconduct or misconduct putting others at risk. It would be unfair to use evidence obtained covertly for minor disciplinary matters.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom. The removal/ cancellation of recording and any findings will also be fully documented.

Any incident of covert recording anywhere within SGUL will be treated as gross misconduct and the appropriate authorities/senior management notified unless authority has been sought and given prior to usage in line with this procedure.

Security Control Centre


The Security Control Centre (SCC) is situated in the Hunter Wing foyer and can receive images from throughout the site. It is staffed 24-hours a day by uniformed University contracted Security Officers. Monitors are not visible from outside the SCC.

The SCC is also linked with uniformed Security Officers and other SGUL Staff who provide mobile and foot patrols of the site and are able to respond to incidents identified on the CCTV monitors.

No unauthorised access to the SCC will be permitted at any time. Access will be strictly limited to the duty security staff, authorised members of senior management, police officers and any other person with statutory powers of entry. A list of those members of senior management authorised to access the SCC is given at Appendix A. Regardless of their status, all A to the control room will be required to sign the visitor's book and a declaration of confidentiality.

Staff, students, and visitors may be granted access to the SCC on a case-by-case basis and only then on written authorisation from Facilities Manager. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the SCC.

Before allowing access to the SCC, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the SCC via the DOB and any visitors granted emergency access. Any other personnel admitted to the control room, such as cleaning staff or engineers effecting repairs must also be authorised by the Facilities Manager or the Director of Estates and Facilities (verbally or in writing) and must be supervised at all times whilst they are in the control room. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

Data Protection

The University is committed to complying with the requirements of the Data Protection Act 1998 and will operate the system in accordance with the eight data protection principles. The University will include the CCTV system on the University's data protection notification.

The Facilities Manager will be responsible for ensuring that the notification covers the purposes for which the system is used.

The standards, which must be met if the requirements of the Data Protection Act 1998 (DPA) are to be satisfied, are based on the eight data protection principles which are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
 - a. at least one of the objectives is met, and
 - b. in the case of sensitive personal data, the correct authority and permissions have been gained.
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

All members of staff involved in operating the system will be made aware of the objectives of the scheme and will be permitted only to use the system to achieve those objectives.


All members of staff involved in operating the system will be forwarded a copy of this policy for reference and compliance purposes.

The University recognises the importance of strict guidelines in relation to access to and disclosure of recorded images and all members of staff should be aware of the restrictions relating to this set out in this Code and the rights of individuals under the Data Protection Act.

Use of the System

Training

All security staff and other authorised users must read this policy prior to being instructed on the operation of the system. All security staff must hold a current and valid CCTV SIA Licence.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

All staff working in the Security Control Centre will be made aware of the sensitivity of handling CCTV images and recordings. All staff are to be fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

Training in the requirements of the Data Protection Act 1998 will be given to all those required to work in the Centre by the Data Protection Officer.

Confidentiality Declaration

Any member of staff, visitor, contractor that enters the SCC MUST sign the CCTV access book, first reading the disclosure declaration at the front of the book.

"In signing this Access Control book, all visitors to the St George's University CCTV monitoring area acknowledge that the precise location of the CCTV monitoring and details of those operating the system, is and should remain confidential. They further agree not to divulge any information obtained, overheard or overseen during their visit."

Should a member of staff/visitor/contract not wish to sign after reading the disclosure declaration, then access will not be permitted to the SCC.

For members of staff or contractors who require prolonged periods of time to the SCC, a separate CCTV confidentiality agreement (Appendix B) can be given, read and signed. Once this agreement has been signed once then the person will not have to sign the CCTV access book every time they enter behind the desk.

Operational

Unless an immediate response to events is required, staff in the CCTV Control Centre must not direct cameras at an individual or a specific group of individuals. Cameras are not to be focussed on private homes, gardens and other areas of private property.

The system can be used to observe the site and areas under surveillance and identify incidents that require a response; the response should be proportionate to the incident being witnessed. On some occasions the deployment of a security officer may be sufficient on other occasions contacting the Police to respond may be the appropriate action. Such surveillance should be in accordance with the stipulated objectives. Whenever a response is required a log should be commenced on the incident report.

Viewing monitors should be pass-worded and switched off when not in use to prevent unauthorised use or viewing.


As community confidence in the system is essential, all cameras will be operational. An appropriate maintenance programme will be established.

Storing and Viewing Images

All images recorded on the University cameras are digitally stored, either centrally in the Security Control Centre or remotely within the local area, on computer/server hard drives and although the images can be searched it is not possible to tamper with or alter them.

In order to maintain and preserve the integrity of the Digital Video Recorder (DVR) Hard Disks used to record events from the CCTV cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to:

- Each DVR must be identified by a unique mark or serial number.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

- Each DVR must be kept in a secure location with access restricted to authorised staff.
- The controller shall check each DVR daily to ensure the system is operational.
- If data material is archived on the system, the reference number must be recorded on the record sheet in the event of the Police requiring images they can be 'burnt' onto a CD/DVD for evidence in court, on receipt of the appropriate receipt of a Data Protection form.

The general CCTV images over-record after 14 -21 days, dependant on the image quality being recorded, however any relevant images can be 'locked' on the hard drive for future reference.

All other images and data will be erased after 31 days unless required for evidential purposes.

Locked images are reviewed on a 3 monthly basis and any not still required for evidential purposes will be deleted.

Viewing of live images on monitors is restricted to security operators with a valid CCTV AI Licence or other authorised person and can only be accessed using passwords.

CCTV Recorded Images may be viewed for authorised demonstration and training.

Disclosure

The following guidelines will be adhered to in relation to disclosure of images:-


- Will be in line with the above objectives for the CCTV system.
- Will be controlled under the supervision of the Facilities Manager
- A logbook/sheet will be maintained itemising the date, time(s), camera, person copying, person receiving and reason for the disclosure.
- The appropriate disclosure documentation from the Police will be filed for future reference.
- Images must not be forwarded to the media for entertainment purposes or be placed on the internet.
- Images will only be released to the media for identification purposes in liaison with the Police or other law enforcement agency.

NB: Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

Subject Access Requests

Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. All such requests are to be handled centrally by the University Planning and Secretariat Department.

- These images must be provided within 40 calendar days of receiving a request.
- A fee of up to £10 is payable (this is the current statutory maximum set by Parliament).
- Those who request access must provide you with details which allow you to identify them as the subject of the images and also to locate the images on your system.
- A log of such request will be maintained in the disclosure log.
- If images of third parties are also shown with the images of the person who has made the access request, consideration must be given as to whether there is need to obscure the images of the third parties.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

Freedom of Information

As a public body the University may receive requests under the Freedom of Information Act 2000 (FOIA). All such requests are dealt with centrally by the University Governance, Legal & Assurance Services.

The response should be made within 20 working days from receipt of the request. Section 40 of the FOIA contains a two-part exemption relating to information about individuals. When a request for CCTV footage is received the following should be considered:-

- Are the images those of the requester? If so, the information is exempt from the FOIA. Instead, this request should be treated as a data protection subject access request as explained above.
- Are the images of other people? These can be disclosed only if disclosing the information in question does not breach the data protection principles.

A Viewing Request Form (Appendix C) is required to be filled out every time CCTV is viewed by anyone except as part of routine operations by SGUL Security staff. It is split into three sections.

- CCTV viewing by Emergency Services during an incident. Permission may be granted by Incident Commander/Gold Team Member or in exceptional circumstances by a Security Supervisor.
- Review of CCTV by any authorised party that relate to a specific security issue or incident. Permission must be gained from Facilities Manager or the Director of Estates & Facilities.
- Review of CCTV involving images (current or recorded) which will involve the monitoring of staff or students either overtly or covertly and could lead to action or investigation by Human Resources, Registry, IT or other SGUL departments. Permission must be gained from Vice Chancellor.

Primary request to view data

Primary requests (i.e. those from law enforcement agencies) to view data generated by the CCTV system are likely to be made by third parties for any one or more of the following purposes:

- Providing evidence in criminal proceedings (Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996),
- Providing evidence for civil proceedings or tribunals,
- The investigation and detection of crime,
- Identification of witnesses.


Major incidents

In the event of a major incident arising, such as serious public disorder, bomb threats/explosions or serious fires the emergency services will be given authority to supervise the CCTV control centre. Such authority will be given by the Director of Estates and Facilities or the Facilities Manager, Emergency Response Team or Incident Commander / Gold Team Member in their absence verbally or in writing.

Third parties

Third parties are required to show adequate grounds for disclosure of data within the above objectives, and may include, but are not limited to:

- Police,
- Statutory authorities with powers to prosecute,
- Solicitors,
- Plaintiffs in civil proceedings,

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

- Accused persons or defendants in criminal proceedings,
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime,
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

Staff / Student Monitoring

The University will only investigate images for use in a staff and student disciplinary case when there is a suspicion of gross misconduct and not to generally monitor activity. In these situations, the investigating person will formally request access to images, where these may prove or disprove suspected potential gross misconduct / serious student discipline cases. The investigator will be referred to the Vice Chancellor to allow permission and a signed CCTV Viewing Request Form filled out. Where access is given, the confidentiality of these images and who is able to access them will be closely controlled.

The following will also have access to CCTV images.

- Staff and Students in connection with disciplinary matters which directly concern them.
- Trade Union representatives only in connection with disciplinary matters which directly concern one of their members (subject to the person's written request and consent).

Release of Images

A record will be maintained of the release of Data on Disk/USB to the Police or other authorised applicants. A register will be available for this purpose. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.


A disk/USB required for evidential purposes must be of the DVD/Encoded USB type only, disks/USB can be released to the police or other authorised third party on production of a signed data access request form or a DIPA. Should a disk be used for the download, each disk should be sealed in its own case using a tamper proof seal. The disk/USB is to be handed to the person making the request on production of positive ID such as Police Warrant Card, Picture ID Card, Driver Licence, etc., the record sheet should then be completed, and the disk/USB signed for and counter signed by the controller.

Disks/USBs will only be released on the clear understanding that the Disk remains the property of the University, and both the disk/USB and information contained on it are to be treated in accordance with this code. The University also retains the right to refuse permission to pass to any other person the disk/USB or any part of the information contained thereon.

The Police may require the University to retain footage for possible use as evidence in the future. Such footage will be saved within the CCTV PC, ready to be downloaded on to disk or USB.

Requests for image disclosure should be made in writing to the Director of Estates and Facilities or the Facilities Manager. Upon receipt of a bona fide request to verify the existence of relevant data the Director of Estates & Facilities or the Facilities Manager will ensure:

- Permission from the Vice Chancellor has been granted where needed,
- No undue obstruction of any third-party investigation to verify existence of data,
- The retention of data which may be relevant to a request,
- That there is no connection with any existing data held by the police in connection with the same investigation.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

The University has discretion to refuse any third-party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once an image has been disclosed to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with the Data Protection Act (DPA) in relation to any further disclosures.

Signage

Signage has been erected at the main entrances to the University and at other locations where CCTV is in use informing that them that CCTV surveillance is in operation. The signs contain details of the University and a contact number for Security. It is the responsibility of the Facilities Manager to ensure adequate signing is erected to comply with the Information Commissioner's Code of Practice.

Breaches of The Code (Including Breaches of Security)

Any breach of the Code of Practice by SGUL security staff will be initially investigated by Facilities Manager or the Director of Estates & Facilities, in order for him/her to take the appropriate disciplinary action.


Any serious breach of the Code of Practice will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried out by Facilities or other nominated individuals.

Complaints


Complaints received in relation to the use of the CCTV system should be made to the Director of Estates and Facilities or the Facilities Manager who will investigate the allegation or complaint and then follow the Estates and Facilities Complaint and Service Issue procedures.

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

Appendix A

Authorised access to Security Control Centre:-

- SGUL's Contracted Security staff
- Vice – Chancellor
- Director of Estates and Facilities
- Deputy Director of Estates and Facilities
- Facilities Manager
- Sports & Residential Services Manager
- Safety, Health and Environmental Assistant Director.
- Incident Commander / Gold Team during a declared incident
- Emergency Response Team Member during a declared incident

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

Appendix B



CONFIDENTIALITY DECLARATION

Please read the following carefully and sign in the presence of a witness:

I, _____, hereby acknowledge that I have been advised that any *unauthorised divulgence of any matter which is ** confidential and which I learn in the course of my duties may be deemed to constitute gross misconduct and may render me liable to instant dismissal.

I hereby undertake that I will make no unauthorised divulgence of any matter of which I become aware in the course of my employment / visit.

- * Any sensitive information requests will have to be authorised by the Management, on a case by case basis.
- ** We define "Confidential" matters as: All information of whatever nature in whatever form, relating to the companies or its clients activities. This includes the activities of its employees that have been obtained or which originates from any source, whether from the public or private sector, including without limitation information received from the company, save and except information which at the time was obtained and was/is in the public domain.

Visitor / Employee Declaration:

Signed: _____

Name (Print): _____


Date: _____


Witness:

Signed: _____

Name (Print): _____

Date: _____

	Estates & Facilities Department		
	Title: CCTV Policy	Author: J.Hollow	Date:02.02.24
	Doc No.: Admin /E&F /EandFDocumentManagement / Facilities /Security /CCTV/ CCTVPolicy	Version: 4	Review Date: 02.02.26

 St Georges, University of London- CCTV viewing request form			
Applicant Information			
Requested By		Position	
Department		Email	
Date		Time	

Emergency Services Request	
Definition	Review of CCTV images (current or recorded) by the police or emergency services during an incident
Date (if known)	
Time (if known)	
Camera / Location (if known)	
Approved By: (Security Supervisor / Incident Control Commander / Gold Team)	

Standard Incident	
Definition	Review of CCTV images (current or recorded) that relates to a minor security issue NOT involving the monitoring of any members of staff or students which could lead to action or investigation by Human Resources, IT or other SGUL departments.
Date (if known)	
Time (if known)	
Camera / Location (if known)	
Justification (explanation as to why the information is requested)	
Approved By: (Director, Deputy Director, Estates & Facilities &/or Customer Services Manager)	

Monitoring of Staff / Students	
Definition	Review of CCTV images (current and recorded) which will involve the monitoring of staff or students AND could lead to action or investigation by Human Resources, Registry, IT or other SGUL departments
Date (if known)	
Time (if known)	
Camera / Location (if known)	
Justification (explanation as to why the information is requested)	
Approved By: (Vice Chancellor or COO)	