Document Title	Management and Use of CCTV Systems
Version	V1.3.1
Author	Head of Facilities and Operations
Owning Department	Estates and Facilities Directorate
Approval Date	02/06/17
Review Date	18/02/19
Approving Body	04 June 2019

1.0 INTRODUCTION

This policy is applicable to all University staff. Its purpose is to ensure that the University Closed Circuit Television (CCTV) system is used to create a safer environment for staff, students and visitors to the University and to ensure that its operation is consistent with the obligations on the University imposed by Data Protection legislation. For the purposes of the Data Protection legislation, the Data Controller is the University of Greenwich.

The University has a CCTV surveillance system installed across its campuses for the principal purposes of preventing and detecting crime and promoting public safety.

The images from the CCTV system are monitored from Security Points at each campus which are staffed by the University's Security Officers. It is recognised that ancillary benefits of operating CCTV for this purpose may include reduction of the fear of crime generally and the provision of a safer public environment for the benefit of those who live or work within and visit the University.

Due to public concern surrounding a surveillance society, the use of CCTV surveillance must be consistent with respect for individuals' privacy. Other methods of achieving the objectives of a CCTV surveillance system will therefore be considered before installation of any CCTV camera on the University campus.

This code complies with the CCTV Code of Practice V1.2 dated 09/06/2017 produced by the Information Commissioner's Office, website: www.ico.gov.uk.

2.0 SCOPE

This policy applies to all University CCTV cameras and equipment installed and maintained by the Estates and Facilities Directorate on the University's Greenwich, Avery Hill, Woolwich and Medway campuses including the use of an Automatic Number Plate Recognition (ANPR) system at Avery Hill. Together, these comprise the University CCTV System. This policy does not apply to 3rd party managed systems e.g. outsourced student accommodation. The University is the Data Controller for this system, determines the purpose of recording and is legally responsible and accountable for its use. This policy will be adapted to apply to all systems for which the University is the Data Controller on all campuses.

Faculties and Directorates wishing to install localised CCTV and surveillance devices are required to seek approval from the Director of Estates and Facilities and the University Data Protection Officer prior to installation. The necessity for such installations will need to be justified in full and a privacy impact assessment and Security Checklist completed to identify how alternative control measures would not be feasible for the area in question. Full details on how the system will be controlled and managed in line with this policy and the ICO CCTV Code of Practice V1.2 dated 09/06/2017 must be provided so that the Director of Estates and Facilities and the University Data Protection Officer can make an informed decision on the proposed installation. Where local surveillance and recording equipment is approved and installed the Estates and Facilities Directorate will not be responsible for the day-to- day management or maintenance of the system and so Faculties and Directorates must ensure that their operating procedures clearly define these responsibilities on a local level.

This policy also covers body worn video cameras and specific arrangements for their use are covered in Appendix 3.

This policy does not apply to audio-visual recordings made by members of the University community or visitors for their own private use on their own personally owned equipment. The University is not the Data Controller for such recordings. However, personal use of audio-visual recordings to harass or cause distress to others may be subject to disciplinary sanctions in accordance with other University regulations and policies governing the conduct of students, colleagues and other users and may also be in breach of criminal law.

3.0 OBJECTIVES

The University of Greenwich uses CCTV at its campuses for the purposes of:

- maintaining security of the premises
- prevention of crime
- investigation of crime
- investigating cases of gross misconduct, as referred to in the University's Disciplinary Procedure
- identification of any behaviour which may put others at risk, as referred to in the University's Health and Safety Policy

The University will only use the images or footage captured by the CCTV system for these purposes. It is not used to proactively monitor individual members of the University or public. If the University has a justified suspicion that a crime may have been committed or may be committed in the future, that the security of its premises may be compromised or that potential act(s) of misconduct or behaviour which puts other at risk may have been committed, it may retrospectively review CCTV footage which has been collected. CCTV cameras will be sited and their manipulation restricted to ensure they do not view areas that are not of interest and are not intended to be the subject of surveillance.

4.0 OPERATION OF THE UNIVERSITY'S CCTV SURVEILLANCE SYSTEM

<u>The System</u>

The system is operational and images are capable of being monitored twenty-four hours a day throughout the year. All CCTV cameras are configured to record images only: any sound recording facilities will be switched off or disabled.

There are CCTV cameras inside the University's buildings, in public areas and in certain external locations at the University's Greenwich, Avery Hill and Medway campuses and at Woolwich. The CCTV system at the Avery Hill Southwood site has vehicle number plate recognition software which is used to assist with the requirement on the University by the Royal Borough of Greenwich to count the number of cars which enter the site. It is not used to monitor the general activities of staff or students. CCTV recordings are motion activated rather than continuous.

The University is committed to fair, lawful, open and accountable use of CCTV. The University will not use CCTV for covert monitoring except in exceptional circumstances in which all of the following conditions are met:

- that there are grounds for suspecting criminal activity or equivalent malpractice such as behaviour which puts others at risk;
- that covert monitoring is the only practical way of obtaining evidence of this malpractice;
- that informing people about the monitoring would make it difficult to prevent or detect such wrongdoing;
- that the camera would be used only for a specific investigation, for a specified and limited time and be removed when the investigation has been completed.

To ensure privacy, wherever practicable, the CCTV cameras are prevented from focusing directly or dwelling on domestic or residential accommodation. CCTV cameras located in or facing student accommodation will be trained on the exterior entrances and communal areas such as corridors and common rooms. Where it is not practicable to prevent the cameras from capturing images of such areas appropriate training will be given to system operators to ensure that they are made aware that they should not be monitoring such areas.

The CCTV equipment and location of each camera will be chosen to meet the quality and image capture standards necessary to achieve the University's purposes for processing the images. The location and technical specification will take account of the field of vision of the camera, light levels and other environmental conditions and minimise the capture of images that are not relevant to the University's purposes. In procuring and deploying CCTV equipment, the University will take account of the technical standards set out by the Home Office Scientific Development Branch so that images are of sufficient quality for the University's purposes. The Home Office and the Information Commissioner's Office recommend that CCTV image quality must be fit for one or more of the following purposes:

a) monitoring: to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.

b) detecting: to detect the presence of a person in the image, without needing to see their face.

c) recognising: to recognise somebody you know, or determine that somebody is not known to you.

d) identifying: to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

CCTV equipment will be maintained and tested in accordance with a regular schedule. The local Campus Facilities Manager or their nominee will be responsible for testing the quality of images to ensure that recorded images and prints as well as live images are clear and fit for purpose, taking account of seasonal variations, such as the growth of spring and summer foliage or other factors that may obscure images, and to check that date and time stamps are correct.

Images captured by cameras will be recorded on equipment located securely within University buildings. The Security Control Room has monitoring equipment which allows Security officers to monitor live images from the cameras, and any transfer of images onto other media will only take place from within the Campus offices in line with this policy. Adequate measures will be taken to ensure that equipment and recordings are

held securely, and that monitors cannot be overlooked by individuals other than security staff.

Although every reasonable effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the areas of coverage.

Each such use of CCTV must be authorised in advance by the Director of Estates & Facilities and recorded in the central log of CCTV use by the local Campus Facilities Manager.

CCTV data will be kept for up to 31 days, unless an enquiry has been made in which case it will be kept separately for as long as necessary (also see Section 6.0).

The public and University community will be made aware of the presence of the system by appropriate signage which sets out the purposes for processing the CCTV images and identifies the University as the Data Controller responsible for processing those images.

Security Control Room

Images captured by the system will be monitored in the secure Security Control Room which is located in the Security office at each of the campuses.

Access to the Security Control Room is limited to the Security Officers and other staff members authorised by the Director of Estates & Facilities. Police Officers may enter with the explicit consent of the Director of Estates & Facilities or the local Campus Facilities Manager. Other persons may be authorised to enter the Security Control Room on a case-by-case basis with the explicit consent of the Director of Estates & Facilities with each visit being supervised at all times.

Details of all visitors will be recorded in the Occurrence Log which is kept in the Security Control Room.

Handling of images and information within the Security Control Room will be carried out in accordance with this policy and Data Protection legislation. The Director of Estates & Facilities will be responsible for compliance with above and for the development of working procedures within the Control Room to ensure such compliance.

5.0 MONITORING OF CCTV IMAGES

The local Campus Facilities Manager will ensure that all staff (including relief/temporary staff) are fully briefed and trained in respect to all functions, both operational and administrative, arising within the operation of CCTV surveillance, including training in the data security requirements of this policy and Data Protection legislation.

The control of the CCTV Surveillance System will always remain with the University. However, at the discretion of the Director of Estates & Facilities or their nominee, the University may act on advice from the police in order to operate cameras during an incident to monitor potential public disorder, assist in the detection of crime or facilitate the apprehension and prosecution of offenders in relation to crime and public order.

6.0 RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

All recording media used for the monitoring and capture of images on the University's CCTV system belong to and remain the property of the University.

The Security Control Rooms are supported by a digital recording system which stores images on appropriate media for up to 31 days or until capacity is reached, whichever is the shorter period, and the images are then automatically erased.

Should it be necessary for images to be retained for release to a third party (including the Police) under the exemptions contained within the Data Protection Act 2018, Schedules 2 - 4, or retained for any other purpose in accordance with this policy, for which the University's use of the system is registered with the Information Commissioner's Office, copies of those images will be transferred to a secure encrypted computer file.

Unless required for any of the reasons contained within these Schedules, recorded images will be retained in the Control Room up to 31 days, after that time the images are automatically overwritten by the recording equipment.

Where applicable, any recording medium will be cleaned before re-use to ensure that images are not recorded on top of images previously recorded.

All media containing recordings will be securely destroyed at the end of their lifespans.

Disclosure

Footage or recordings of individuals who can be identified from the image are personal data as defined by Data Protection legislation. Requests to view footage or receive copies of recordings of CCTV should be made to the local Campus Facilities office staff or to the Data Protection Officer, both of whom will consult with the Director of Estates and Facilities Management (or nominee) on disclosure. Security staff receiving requests should refer them to the local Campus Facilities Manager. Requests should always be made in writing, regardless of who is requesting the data.

Personal Data

If an individual requests to view footage or receive a copy of a recording of CCTV of their own personal data, this should be treated as a Subject Access Request under the Data Protection Act. This is regardless of whether the individual is a member of staff, a student or a member of the public. This request should be made in writing to the local Campus Facilities Manager who will consult with the Director of Estates and Facilities Management (or nominee) and the Data Protection Officer on disclosure, accompanied by proof of identity (for list of relevant personnel see 9.0 below). There is a form available for use (Appendix 1, Form: CCTVform.001).

The individual must provide details which will allow the University to identify them as the subject, and how to locate them on the system. This may include a photograph of themselves, a description of what they were wearing at the time, and the date, time and location of the incident.

If the University finds that identifiable third parties appear on footage at the same time as the subject, it may decide that footage will not be disclosed, as set out in Section 40(2) of the Freedom of Information Act 2000 which refers to disclosure of third-party personal data. The obscuring of certain images on the system is not possible.

If the University is satisfied that data may be disclosed the individual will be provided with a digital copy of the footage within one calendar month of receiving a request.

Staff, students, members of the public, or external organisations or bodies who make requests for third party CCTV data, should make their request in writing to the local Campus Facilities Manager or to the Data Protection Officer who will consult with the Director of Estates and Facilities Management (or nominee) on disclosure. There is a

form available for this (Appendix 2, form CCTVform.002). The police will not need to make a request if the University has formally contacted them regarding an incident. They will however be required to make a formal request if they have been contacted by a third party, including a member of the University acting in their personal capacity regarding an incident on or adjacent to the Campus.

The University will make decisions on a case by case basis, and according to the terms of the Freedom of Information Act, as to whether to disclose third party CCTV data. It may disclose in the following instances:

- For the prevention or detection of crime
- In some limited circumstances where the needs of the requester outweigh those of the individual whose image was recorded.

The University will take into consideration whether there is any risk to the safety of any people involved.

Any requests for data for footage of the University of Kent buildings at Medway should be made to the University of Kent.

Incidents

If an incident has taken place which has been recorded on CCTV which could be classed as a crime or as a possible breach of University rules and regulations, the following personnel are allowed to view footage as a matter of course:

- Local Campus Facilities Managers and/or Deputy Campus Facilities Managers
- Other senior Estates and Facilities Management staff or staff directly involved in any investigation
- Security personnel
- The University's Data Protection Officer (or nominee)
- The police (if the University has invited them to)

If necessary, an image in the form of a still may be produced for the purposes of identifying individuals or for the purpose of investigating the possible breach or crime. This image may be shown to key staff who in the opinion of those mentioned above may be in a position to identify the individual or further the investigation. Copies of the images may be burnt on to a DVD for purposes of a disciplinary enquiry. All such copies must be returned to the local Campus Facilities Manager at the end of the disciplinary action for retention or destruction.

Images will not be made public in the following ways:

- By making posters for display in a public place
- On the internet or University intranet
- By circulating in any electronic format

Images may be displayed in semi-public places such as private offices or gatehouses, in exceptional circumstances.

The University may involve the police at any stage should it see fit to do so and will provide the police with CCTV footage if necessary. It may require the police to make a formal request for data, if it has not contacted them itself.

Records

The following records will be kept by the local Campus Facilities Manager:

- CCTV footage (up to 31 days)
- Maintenance records (two years)
- Log of requests for data (six years)
- Disclosure details and digital CCTV copies of footage of incidents which have been formally investigated by the University (six years)

Destruction

Digital copies of CCTV footage will be confidentially destroyed by the local Campus Facilities Manager.

7.0 COMPLAINTS/BREACHES

Breaches of this policy, whether by security staff, or other staff monitoring the system, or who have access to the monitored images, or who access images without authority to do so, will constitute Gross Misconduct and will result in disciplinary action being taken, which may lead to dismissal under the University's Disciplinary Code, Policy and procedures.

It is also recognised that other members of the University or third parties may have concerns or complaints in respect to the operation of the CCTV Surveillance System. Any concerns or complaints should, in the first instance, be addressed to the Director of Estates and Facilities who will follow the University Complaints Policy.
Concerns or queries relating to any aspect of compliance with Data Protection legislation, should be directed to the Data Protection Officer.

8.0 RESPONSIBLE OFFICER

The Director of Estates and Facilities is responsible for the implementation of this policy, in consultation with the Data Protection Officer.

Contact details of Senior Facilities Management staff and the University's Data Protection Officer:

Director of Estates and Facilities/ Head of Facilities and Operations
University of Greenwich
51 Aragon Court
Avery Hill Road
London SE9 2UG
Tel: 020 83319232

Data Protection Officer
University of Greenwich
Queen Anne Court
Old Royal Naval College
London SE10 9LS
Tel: 020 8331 8860

Campus Facilities Manager/Deputy – Avery Hill Campus
University of Greenwich
Facilities Management Office
Flat 46 Aragon Court
Avery Hill Road
London SE9 2UG
Tel: 020 8331 8848

Campus Facilities Manager/Deputy – Greenwich Campus
University of Greenwich
Queen Anne Court
Old Royal Naval College
London SE10 9LS
Tel: 020 8331 7701

Campus Facilities Manager/Deputy – Medway Campus
University of Greenwich Facilities Management Office Pembroke
Central Avenue Chatham Maritime
Kent ME4 4TB
Tel: 01634 883 039

Further Reference

This policy has been developed to comply with the General Data Protection Regulation and Data Protection Act 2018 and the Information Commissioner's Office CCTV Code of Practice, 2017

Appendix 1 - Request Form - CCTVform.001 (there are two pages to this form)

UNIVERSITY OF

GREENWICH DATA

PROTECTION

Request for Access to Personal CCTV Data

I, _____

wish to have access to Personal Data that the University of Greenwich has about me which is held as CCTV data.

Description of event, including date, time (start and end time if known) and location (to include building, and room number/area):

.....

.....

.....

I enclose a copy of a photo proof of identity (passport or UK driving licence) and a passport sized photograph of myself. I understand that I will receive a formal response from the Estates & Facilities Management Office or Data Protection Officer within one calendar month of my request being received, subject to all the necessary supporting documentation having been submitted with my original request. I understand and accept that I must personally collect any CCTV footage the University releases under this request, at which time I must produce an original photo proof of identity.

Signed:

Date:

Name (Block Capitals):

Directorate / Faculty (Capitals):

Date of Birth:

Student / staff no. (if known):

Address:

Telephone:

Hand or send this form, fee and supporting documents to the local Campus Facilities Manager on the relevant University Campus or their Deputy. In their absence this form should be sent to the: Head of Facilities and Operations or Director of Estates & Facilities Management or Data Protection Officer (see Section 9.0 of the University's CCTV Policy, or ring the main switchboard on 0208 331 8000 for contact details).

I confirm receipt of the CCTV footage outlined above.

Signed

Date:

Office Use

Ensure identity checked and copy of evidence produced to confirm identity is attached:

Signed:

Date

Appendix 2 - Request Form - CCTVform.002 (there are three pages to this form)

Requests to the University of Greenwich for CCTV footage from third parties.

The University of Greenwich tries to ensure the best balance between providing appropriate information or evidence for investigating authorities, and protecting individuals or organisations. We will assess whether our co-operation is necessary and proportionate before we agree or refuse to provide the information you request. It is mandatory for you to provide certain information before we will consider your request.

Is your request for the detection or prevention of crime (please tick the relevant box below: (this section must be completed)		
	YES	NO
If yes, please give details on why the requested CCTV is relevant. A decision on whether to release CCTV footage will be made taking into consideration your response to this question.		
If no, please specify why you are requesting CCTV footage. A decision on whether to release CCTV footage will be made taking into consideration your response to this question.		

Details of CCTV footage requested:

Date of incident:	Name of person(s) involved, and name and/or description if known:	For Office purposes only:
Building:	Room/Area:	Time/Duration:

Your details:

Date of request:	**Name:**
ID Number and Company Name:	**Signature:**

Send this form to the local Campus Facilities Manager on the relevant University Campus or the Deputy. In their absence this form should be sent to the: Head of Facilities and Operations or Director of Estates & Facilities Management or Data Protection Officer (see Section 9.0 of the University's CCTV Policy, or ring the University's main switchboard on 0208 331 8000 for contact details).

Office use only: Data Received:
Date sent for Authorisation:
Person sent to for Authorisation:

I give my approval/do not give my approval to release the CCTV as noted above. Name: Signature: Date

Incident Ref no:	Master CD/DVD no:	Copy CD/DVD no:

Office Use

Ensure identity checked and copy of evidence produced to confirm identity is

attached: Signed: Name: Job Title:

Campus:
Date:
Please sign below to confirm:

I have received the above data from the University of Greenwich's CCTV system, and I confirm that it will be held in accordance with Data Protection legislation, and that it will not be used in any way incompatible with the purpose for which it is being disclosed.
Signed:..... Date.....

CCTV images remain the property of the University of Greenwich. Under no circumstances should copies be taken or their contents broadcast without the written agreement of the University's
Data Protection Officer.

Appendix 3

Arrangements for the Use of Body Worn Video Cameras (BWV)

Body worn video cameras (BWV) are CCTV cameras attached to the uniforms of security staff. These cameras recorded both audio and visual footage
Purposes of BWV
BWV are used at the University of Greenwich to enable the recording of incidents where video footage will be beneficial to:

- increase reassurance of members of the University community;
- reduce crime and disorder and the fear of crime and disorder;
- reduce antisocial behaviour;
- ensure that the University campuses is a safe and secure environment to work and study;
- increase the safety of security staff;
- reduce escalation of incidents; and
- resolve complaints about security incidents and disciplinary procedures, internally, and prosecutions, externally, more quickly.

Principles of Use

- Body worn video cameras (BWV) should only be used by University of Greenwich security staff (which includes security contractors): any change to this arrangement must be agreed by the Vice Chancellor or another member of the Executive Team.
- All BWV shall be managed by the University of Greenwich security team. Local security managers shall be responsible for the use and for training of staff in its use.
- All staff who may use BWV will have full training in their use. No staff will be permitted to use BWV until they have agreed to these principles, confirming their receipt, reading and understanding.
- All incidents which involve the use of body one cameras shall be logged on the AMS, documenting the date, time, reason for use and name of the officer wearing the BWV.

The officer wearing BMV is always responsible for its use. Before recording commences officers wearing BWV should alert those present that the recording will be taking place stating the following:

- that recording is taking place;
- that it includes audio recording;
- their own name;
- the date;
- the time;
- the location;
- and the nature of the incident.

If the recording has started prior to the arrival of the officer at the scene, they should state this upon arrival.

Where this is not operationally possible, this information should be provided as soon as it is practicable to do so.

- The cameras shall be aimed at those involved in the incident and not at third parties who are not involved. Officers should do their best to ensure that those not involved in an

incident are not recorded: this may include standing in a position to block them from being filmed or asking them to move.

- BWVs should be permitted to continue for approximately 15 minutes after any incident has concluded the officer wearing the BWV should state the date, and time.
- BWVs should never be used covertly or concealed.
- The security will use a documented BWV footage management system; this system will be compliant with all relevant legislation and provide a full audit trail for the footage to ensure its evidential value.
- Footage will be retained for 31 days unless required for the purposes of an investigation.
- Every six months, use of BWV shall be reviewed and the BWV footage management system will be audited.

I confirm that I have been trained in the use of Body Worn Video Cameras and have received, read and understood a copy of these arrangements for its use:

Name	
Date	
Signature	
Training given by	