Estates & Facilities Directorate

UNIVERSITY OF GREENWICH

CCTV and Video Surveillance Policy

Version	V3.2024.1
Author	Associate Director of Campus Management
Owning Department	Estates & Facilities Directorate
Approval Date	02/06/2017
Review Date	15/11/2024
Approving Body	Estates and Facilities Management Board

1. Introduction

This policy is applicable to all University of Greenwich staff. Its purpose is to ensure that all university Closed Circuit Television (CCTV) and video surveillance systems are 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 aligns with the guiding principles of the Surveillance Camera Code of Practice 2013, updated 2021.

2. 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. This includes the use of an Automatic Number Plate Recognition (ANPR) system at Avery Hill. Together, these comprise the university CCTV System. This policy applies 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 Executive Director of Estates & Facilities and the University Information Compliance Team 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 the Information Commissioner's Office (ICO) Video Surveillance Guidance. must be provided so that the Executive Director of Estates & Facilities and the University Information Compliance Team 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. 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
- To assist the Royal Borough of Greenwich with car traffic monitoring

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. Operation of the University's CCTV Surveillance System

The System

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 of Greenwich 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.

CCTV equipment will be maintained and tested in accordance with a regular schedule. The Campus Management Team (greenwichfacilities@gre.ac.uk) 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 Executive Director of Estates & Facilities. Such authorisation shall be in consultation with or on the advice of, the Information Compliance Team where necessary and recorded in the central log of CCTV used by the Campus Management Team.

CCTV data will normally be kept for 31 days except where there are unavoidable technical issues, 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 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 Executive Director of Estates & Facilities. Police officers may enter with the explicit consent of the Executive Director of Estates & Facilities or the Campus Management Team. 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 supervised.

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 Executive 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. Monitoring of CCTV Images

The Campus Management Team, including relevant personnel providing outsourced services, 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 Executive Director of Estates & Facilities or their nominee, the university may act on advice from the police 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. 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 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 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 lifespan.

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 Campus Management Team or to the University Information Compliance Office, both of whom will consult with the Executive Director of Estates & Facilities (or nominee) on disclosure. Security staff receiving requests should refer them to the Campus Management Team (Greenwichfacilities@gre.ac.uk). 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 Campus Management Team who will consult with the Executive Director of Estates & Facilities (or nominee) and the Information Compliance Office on disclosure, accompanied by proof of identity (for list of relevant personnel see 9.0 below). There is a form available for use Data Access Requests CCTV and Access Control (office.com).

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 the Data Protection Act 2018 which refers to disclosure of third-party personal data, if it is not possible to do so without materially prejudicing another individual's data privacy rights. 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.

If disclosure by providing a copy is not possible, the Campus Management Team may instead offer for the individual to attend university premises and view the footage, if this would cause less prejudice to another person's data privacy rights. The Campus Management Team may require the individual viewing the footage to confirm in writing that they will not do anything which would interfere with another person's data privacy rights.

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 Campus Management Team or to the Information Compliance Office who will consult with the

Executive Director of Estates & Facilities Management (or nominee) on disclosure. There is a form available for this Data Access Requests CCTV and Access Control (office.com). For verification purposes, we will require an incident reference number to be included in any request for footage. 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 Data Protection Act 2018 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:

- Campus Management Team
- Other senior Estates and Facilities staff or staff, including contractor staff, directly involved in any investigation
- Security personnel
- The University's Information Compliance Office (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 able 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 Campus Management Team 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 Campus Management Team:

- CCTV footage (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 Campus Management Team.

7. 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 Executive Director of Estates & 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 Information Compliance Office.

8. Responsible Officer

The Executive Director of Estates & Facilities is responsible for the implementation of this policy, in consultation with the Information Compliance Office.

Contact details of senior campus management staff and the University's Information Compliance Officer:

Executive Director of Estates & Facilities / Associate Director of Campus Management
51 Aragon Court, Avery Hill Road, London SE9 2UG

Head of Campus Management, Avery Hill Campus
Head of Campus Management, Greenwich Campus
Head of Campus Management, Medway Campus

Greenwichfacilities@gre.ac.uk

University Information Compliance and Accessibility Officer
Complianceteam@gre.ac.uk University of Greenwich, Queen Anne Court, Old Royal Naval College, London SE10 9LS

Further Reference

This policy has been developed to comply with the UK General Data Protection Regulation and Data Protection Act 2018 and the Information Commissioner's Office video surveillance guidance