Closed Circuit Television (CCTV) Policy

1. Introduction

The University of Cumbria uses Closed Circuit Television (CCTV) and body worn cameras within the University premises for the purposes of the prevention and detection of crime and to recognise and identify individuals with a view to taking appropriate action. This policy sets out the accepted use and management of CCTV equipment and images to ensure the University complies with the Data Protection Act 2018 and other relevant legislation. The University processes personal data in line with our Data Protection Policy.

The University is also cognisant with the guiding principles of the Surveillance Camera Code of Practice (2021) as published by the Home Office. The Policy aims to achieve a balance between safety and security of individual and property, and the protection of individual human rights.

2. Purpose

This policy will serve to encourage employees, students, partners, contractors, and visitors of the University to act in a safe manner and comply with all relevant policy. The policy sets down the framework by which management and all employees, students, partners, contractors, and visitors will be expected to meet their duties.

3. Scope

This policy relates to all CCTV systems owned, leased, managed, or controlled by the University. These systems include moveable CCTV surveillance cameras without sound recording and Body Worn Video Cameras (BWVC) with sound recording.

The systems are operated and managed by the Estates and Property Department in conjunction with the approved security contractor.

4. Policy

The University of Cumbria will ensure that the CCTV and BWVCs will be managed in compliance with the appropriate legislation, guidance, and best practice standards.

In doing so, the University will ensure that we deploy CCTV and BWVCs to:

- Promote a safe community and monitor the safety and security of premises
- Assist in the prevention, investigation, and detection of crime
- Assist in the apprehension and prosecution of offenders, including using the images as evidence in criminal proceedings
- Assist in the investigation of breaches in code of conduct and policies by staff, students, and contractors and where appropriate, investigating complaints.

5. Policy Principles

CCTV Cameras: CCTV cameras will be sited in prominent positions where they are clearly visible. Reasonable efforts will be made to ensure that areas outside of the University premises are not recorded. Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

CCTV should not be placed in areas where individuals have an expectation of privacy, such as changing rooms or toilets.

Body Worn Video Cameras: BWVC are routinely used by security staff whilst on duty and recording will only take place when there is a valid reason for doing so.

Individuals are likely to have a strong expectation of privacy in places not generally open to the public. In such circumstances, clear justification for the use of BWVC will be required. BWVC should not be used in private spaces, such as toilets or changing rooms unless there is a compelling need related to the physical safety of staff or others.

All staff must be suitably trained prior to carriage and use of BWVC.

Individuals subject to recording by BWVC will be made aware that it is in use by the security staff making a verbal announcement unless circumstances prevent that from happening.

6. Roles and Responsibilities

Business Assurance Board
Approves the policy, ensuring that support and resource is available to staff for implementation.

Data Protection Officer
Responsible for:

- maintaining the policy and ensuring compliance with Data Protection Legislation
- responding to requests to view footage, as set out in Appendix 2.
- training the Responsible Persons in the appropriate release of any footage as set out in appendix 2.

The Head of Estates and Property
Responsible for ensuring that the system is operational and that there are Responsible Persons in post who are appropriately trained on the system's operation.

The Estates Managers and Electrical Services Engineer (Responsible Persons)
Responsible for the control of CCTV operations and for day-to-day management of the system.

Responsible for viewing of footage, as required, and agreeing to its release as set out in Appendix 2.

Appointed Security Contractors
Responsible for security duties as defined in contractual assignment instructions including CCTV monitoring and use of body worn cameras.

7. Related Policies and Procedures

University of Cumbria:

- Data Protection Policy
- Information Security Policy

Legislation / Guidance:

- Data Protection Act 2018
- Surveillance Camera Code of Practice (2021)

8. Publication, Implementation & Review

This policy shall be approved by the Business Assurance Board. It will be located within the Data Protection area of the Vice Chancellor's Office mini-site on SharePoint and linked to from the Policy Hub.

The policy will be reviewed every three years or following any significant incidents or changes in legislation to ensure it remains effective and up to date.

9. Appendices

Appendix 1: Definitions
Appendix 2: Data Protection Legislation and operation of the Policy

10. Document Control Information

Document Name	CCTV Policy
Owner	University Secretary, VCO
Document Location	VCO Mini-site, Policy Hub
Lead contact	Data Protection Officer, gdpr@cumbria.ac.uk
Approved By	Business Assurance Board
Latest Approval Date	December 2024
Date for Next Review	December 2027
Related University Policy Documents	University of Cumbria Data Protection Policy University of Cumbria Information Security Policy
Version Number & Key Amendment	New policy v1
For Office Use – Keywords for search function	Closed Circuit Television CCTV

Appendix 1: Definitions

For the purposes of this CCTV Policy, the following terms have the following meanings:

CCTV: means cameras designed to capture and record images of individuals and property.

Data: means information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data Controllers: means those people who, or organisations which, determine the manner in which any Personal Data is processed. They are responsible for establishing practices and policies to ensure compliance with the applicable law. The University is the Data Controller of all Personal Data used in during business practices

Data Processors: means any person or organisation that is not a Data User (or other employee of a Data Controller)

Data Subjects: means all living individuals about whom the University holds Personal Data because of the operation of its CCTV.

Data Users: means employees whose work involves the Processing of Personal Data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data Users must protect the Personal Data they handle in accordance with this CCTV Policy.

Personal Data: means data relating to a living individual who can be identified from that data (or other data in the University's possession). This will include video images of identifiable individuals.

Processing: is any activity which involves the use of Personal Data, including obtaining, recording, or holding data, or carrying out any operation on the Personal Data including organising, amending, retrieving, using, disclosing, or destroying it. Processing also includes transferring Personal Data to third parties.

Surveillance Systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

Appendix 2: Operation of the Policy

Personal Data
CCTV and BWVC recordings are covered by the applicable data protection legislation, as information about individuals is recorded such as their images or vehicle registration numbers.

The University is the data controller and must comply with data protection legislation when processing personal data. This includes recording, transmitting, storing and any disclosures.

Data Protection Impact Assessment
Prior to the installation of any new CCTV camera, or system, a Data Protection Impact Assessment (DPIA) will be conducted to ensure that the proposed installation is compliant with data protection legislation requirements.

Unless there is a material change in risk, existing CCTV cameras and systems will be reviewed, and a DPIA carried out at least every three years.

Subject Access Requests
Individuals may request a copy of their personal information, and this may include CCTV recordings. These are referred to as Subject Access Requests (SAR) and can be submitted either verbally or in writing.

All SARs for CCTV footage should be made using the Data Subject Access Request Form (under Right of Access) with appropriate identity to enable the individuals to be identified. Requests will be handled by the Information Governance Team in accordance with the University's Data Protection Policies.

Requests for CCTV for internal purposes
Requests to view CCTV or BWVC footage for internal purposes, for instance in relation to a disciplinary investigation, should be made to the Data Protection Officer clearly setting out why the request is being made and how it might assist the investigation.

Disclosure in emergency situations
An emergency is one where there is a reasonable belief that there is a life-or-death situation or a significant risk of serious harm (either to a staff member, student, or any other person).

Where information is required in an emergency, the Responsible Persons should be contacted and the relevant recordings will be released, subject to the Responsible Persons confirming the identity of the requestor e.g. Police number, before providing any personal data.

Where personal data is disclosed, the Responsible Persons should make a record of the enquiry, and the information disclosed. The record should be passed on to the Information Governance Team.

Disclosure to Third Parties
Requests received from third parties, including law enforcement agencies, for CCTV footage will be handled in conjunction with the Information Governance Team. Any requests for CCTV footage from third parties including law enforcement agencies should be sent to gdpr@cumbria.ac.uk and footage will only be released upon receipt of an appropriate Data Protection request form.

Management and Access
The CCTV system will be operated and maintained by the University of Cumbria Estates and Property Department, in conjunction with the University's approved

security contractor. The CCTV system is checked daily to ensure that it is operating effectively.

The University has Responsible Persons with control of CCTV operations.

The Responsible Persons are:

- Estates Manager (North, Central and South)
- Electrical Services Engineer

The viewing of live CCTV images will be restricted to Appointed Security Contractors or Responsible Persons who will ensure that, in doing so, the purposes of this policy are satisfied.

Storage and Retention of Images
Images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded. Recorded images are stored for a period of no more than 28 days unless there is a specific purpose for which they are retained for a longer period.

The University of Cumbria will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of recorded images. The measures in place include:

- CCTV recording systems are in areas with restricted access
- The CCTV system being password protected
- Restriction of the repositioning of cameras to the authorised persons only
- Restriction of the ability to make copies to the Responsible Person

Incidents
Incidents observed by the Appointed Security Contractors and judged potentially useful for investigative and evidential purposes must be notified promptly to the Responsible Person, who will then determine whether they should be preserved *(i.e., recording made).* These will include any instances where there appears to be threat or harm to person or property.

Images can only be copied and retained with the authority of the Responsible Person who will determine the method of recording, whether any masking is necessary to protect the privacy of other parties.

Original recordings from which copies have been made must be segregated from operational recordings and held securely, accessible only to those directly concerned with the objectives of the system. Images will be deleted upon official closure of any investigation.

The police should be contacted if the Appointed Security Contractors note any 'live' incident that may need their assistance. The Appointed Security Contractors must alert the Responsible Person to such incidents as soon as possible. The Responsible Person will report any such incidents promptly to relevant staff e.g. the Director of Student Services.

Covert Monitoring
Covert monitoring means monitoring designed to ensure that those subject to it are unaware that is taking place; such monitoring should only be used in exceptional circumstances. Covert monitoring may be used when:

- There is sufficient justification to suspect that criminal activity or serious malpractice is taking place, and the issue cannot be resolved in a less intrusive way.

- If covert monitoring is justified, it must be authorised by the University's Data Protection Officer
- It must be targeted, for a limited period and have specific objectives

Misuse of CCTV Systems
The misuse of CCTV systems could constitute a criminal offence. Any member of staff who breaches this policy may be subject to disciplinary action.