THE UNIVERSITY of EDINBURGH

Appendix 1

Closed Circuit Television (CCTV) Policy

1. Policy Statement

1.1. The University of Edinburgh owns a CCTV System (defined in section 5.1 below) which includes over 700 cameras, located across all 5 main campuses, and University accommodation. Cameras are located both externally and internally to protect University property. The CCTV System operates, and is monitored 24 hours a day, 365 days a year and records material in both digital and analogue form.

1.2. The principal purpose of the CCTV System is:

1.2.1. for the prevention, reduction, detection, and investigation of crime and other incidents;
1.2.2. to reduce anti-social behaviour;
1.2.3. to identify any incidents that require a routine or emergency response;
1.2.4. to protect property;
1.2.5. to reassure, and ensure the safety of staff, students, and visitors; and
1.2.6. to support University research and for the protection of animals.

1.3. As a result of the operation of the CCTV System, recorded material can also be used for certain secondary purposes because it is available:

1.3.1. to support legal proceedings;
1.3.2. to assist in the investigation of suspected breaches of University regulations by staff or students;
1.3.3. to support insurance claims;
1.3.4. to assist with health and safety investigations; and
1.3.5. to allow vehicle access control for security purposes

1.4. Secondary monitoring of the CCTV System will be subject to the agreements between the University and authorised partnership agencies and/or the completion of relevant and authorised Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) documentation.

1.5. The use of the CCTV System for any other purpose must be approved by the Director of Estates and the Security Manager, in consultation with the University Data Protection Officer and the Director of Human Resources.

2. Scope

2.1. This policy and the associated CCTV Protocols govern the installation and operation of all CCTV on University premises including fixed, mobile, body worn and Automatic Number Plate Recognition (ANPR) systems.

2.2. It applies to all University of Edinburgh employees, students and contractors employed on University property. Visitors and other members of the public may also be captured by the CCTV System.

2.3. This policy does not include the cameras that have been installed for lecture recording which are covered by the Lecture Recording Policy or cameras that are used for virtual teaching which are covered by the Virtual Classroom Policy.

3. Principles

This policy is underpinned by the following principles:

3.1. The CCTV System will always be used for a specified purpose and be necessary to meet an identified pressing need.

3.2. The CCTV System will be operated with due regard for the privacy of the individual and the University's legal obligations with regular reviews to ensure its use remains justified.

3.3. The University will be as transparent as possible regarding use of the CCTV System, will publish appropriate signage in the locality of CCTV cameras and will publish information about how to find further information or make a complaint.

3.4. The CCTV System will be operated in accordance with documented procedures in which responsibilities are clear, and these are effectively communicated to all relevant employees.

3.5. CCTV images captured by the CCTV System will not be stored for longer than is necessary and will be appropriately secured to safeguard against unauthorised access or use.

3.6. Access to retained images and information is restricted with clear rules on who can gain access and for what purpose such access is granted; the disclosure of images and information will only take place when it is necessary for such a purpose or for law enforcement purposes.

3.7. Any camera, (other than body warn cameras), with the ability to make audio recordings will have this facility switched off.

3.8. CCTV operators will receive appropriate training in the operation of the system, the legal requirements associated with it, and any relevant procedures and policies.

3.9. The CCTV System will have effective and routine review and audit mechanisms to ensure legal requirements, policies and standards are complied with.

3.10. To ensure potential information security vulnerabilities are not exploited, where practical all CCTV equipment will be maintained to the most current versions of software and firmware and, as required, subject to information security testing.

3.11. All images recorded by the CCTV System remain the property and copyright of the University

4. Roles and Responsibilities

4.1. **University Executive** will receive and approve updates to this policy.

4.2. **The Director of Estates** will oversee the implementation of the policy and ensure that it is reviewed regularly.

4.3. **The Security Manager** is responsible for the management and operation of the main Security CCTV System, including installations, recording, reviewing, monitoring, and ensuring compliance with this policy. They will also ensure records are kept, that Local CCTV System Managers are complying with the requirements in this Policy.

4.4. **Local CCTV System Managers** are responsible for the management and operation of their CCTV system, including installations/ maintenance, system management, download management, signage, DPIAs and ensuring compliance with this policy.

4.5. **System Operators -** are University employees that operate the CCTV System. They will have:

- access to CCTV footage and images in order to fulfil their role;
- may be required to access the CCTV System and download evidence where it is required for the management of incidents;
- will undertake relevant training prior to viewing any images on CCTV systems.

4.6. **University Data Protection Officer** will ensure that the University policy complies with Data Protection legislation and will review and sign-off completed DPIAs.

5. Definitions

5.1. **CCTV System -** means the surveillance items including cameras and associated equipment for monitoring, transmission and controlling purposes operated by the University (including the main Security CCTV System, all Local CCTV Systems, automatic number plate registration systems, mobile cameras and BWCs). The term will also encompass the capability for effectively capturing data, in any medium, so it can be viewed or processed.

5.2. **Mobile cameras –** cameras that can be deployed for a temporary period of time which once operational are to be considered part of the CCTV System and which must meet the requirements outlined in this policy

5.3. **Body Worn Cameras (BWC) -** small, visible devices worn attached to clothing (usually on the chest). They're used to capture both video and audio when security staff are attending all types of incidents.

5.4. **CCTV Control Room -** the secure area where CCTV is monitored and where data from CCTV can be retrieved, reviewed and processed.

5.5. **Automatic Number Plate Recognition (ANPR)** - used to read and store data on registration plates at controlled points. These are to be treated as part of the CCTV System including the management of captured data.

5.6. **Incident -** is an activity that raises concern which requires the CCTV System to be reviewed/checked in a targeted way. Incidents will normally be a concern for the safety or security of an individual or property, a suspected criminal offence which is about to take place, is taking place or has taken place, or any occurrence that requires the attention of, or warrants specific action by, the operator.

6. Documentation and Signage

To support the operation of the CCTV System the following documentation will be in place:

CCTV Protocol

6.1. The CCTV protocol provides further details of the rules under which the CCTV System will operate. This includes:

6.1.1. System description
6.1.2. Installation and maintenance procedures
6.1.3. Signage
6.1.4. Training requirements
6.1.5. Privacy requirements
6.1.6. Accessing Live Data
6.1.7. Management of Recorded Data
6.1.8. Retention and Disposal of Data
6.1.9. Complaints

Body Worn Camera (BWC) Protocol

6.2. The BWC protocol provides further details of the rules under which the University BWC system will operate. This includes:

6.2.1. System description
6.2.2. Privacy requirements
6.2.3. System security
6.2.4. Carriage and activation
6.2.5. Reporting and Recording
6.2.6. Training
6.2.7. Health and safety
6.2.8. Procurement
6.2.9. User Guidance

Design Guidelines

6.3. The Estates Department publishes design guidelines for the CCTV Systems. This document lists the criteria for the design, installation and maintenance of the system. It also lays down the requirements and design principals for the CCTV installation company, University Estates design team and the Information Services department.

Data Protection Impact Assessments (DPIA)

6.4. A Data Protection Impact Assessment will be completed for all parts of the CCTV Systems and BWC used within the University to ensure that the CCTV System complies with data protection principles.

Operational Guidance Manual

6.5. An Operational Guidance manual will be in place at the location of all parts of the CCTV System to provide instructions for all System Operators in all aspects of the day to day operation of the system. There will be a separate operational guidelines document for BWCs.

Local System Guidelines

6.6. All local parts of the CCTV System must be registered with the Security control room. The following information will be required as part of this registration:

6.6.1. Monitor, camera and digital video recorder locations.
6.6.2. Local CCTV System manager and system operators.
6.6.3. Local operation guidelines.

6.7. A yearly inspection of local parts of the CCTV System is to be completed by the security team.

Asset Register

6.8. An Asset Register will be held in the Security Operations room detailing each site where aspects of the CCTV Systems are installed and the equipment that is installed in each location.

6.9. Records will also be kept of all:

6.9.1 Trained and Authorised Personnel
6.9.2 Authorised Visitors/Contractors
6.9.3 Approved CCTV Contractors

Signage

6.10. University branded signs will be displayed in the locality of all cameras and include the following information:

6.10.1. The presence of monitoring and recording devices.
6.10.2. The ownership of the CCTV System.
6.10.3. Contact details for further information how to make a complaint.

6.11. These signs are to be located in all areas that are viewed by cameras, in an obvious location.

6.12. Body worn cameras are to be clearly visible, have obvious markings to indicate that they are cameras, and have a warning light to indicate they are recording. A verbal warning is also to be given, when possible, before they are used.

7. Links to Other Relevant Policies, Guidance and Legislation

University Policies and Guidelines

7.1. The following University policies and guidelines may be relevant to the operation of this policy:
7.1.1. Code of Student Conduct
7.1.2. Data Protection Policy
7.1.3. Disciplinary Policy
7.1.4. Freedom of Information Procedures
7.1.5. Lecture Recording Policy
7.1.6. Virtual Classroom Policy
7.1.7. Information Security Policy
7.1.8. Records Management Policy Framework

External guidance

7.2. The following guidance has been reviewed and considered in the preparation of this policy and the associated Protocols:
7.2.1. A National Strategy for Public Space CCTV in Scotland (Scottish Government)
7.2.2. In the picture: A data protection code of practice for surveillance cameras and personal information (Information Commissioner's Office)
7.2.3. Surveillance Camera Code of Practice (Home Office)

Relevant Legislation

7.3. The following legislation is relevant to the University's operation of the CCTV System and considered in the preparation of this policy and the associated Protocols:
7.3.1. Criminal Procedure (Scotland) Act 1995
7.3.2. Data Protection Act 2018
7.3.3. Freedom of Information (Scotland) Act 2002

7.3.4. Human Rights Act 1998
7.3.5. Regulation of Investigatory Powers (Scotland) Act 2000

8. Policy History and Review

8.1. Approved date:
8.2. Approved by:
8.3. Date of next review: December 2024