Appendix 2

University of Edinburgh - Closed Circuit Television *(*CCTV) Protocol 2021

1 Introduction

1.1 The University of Edinburgh uses CCTV to enhance the safety and security of staff, students and visitors across the University Estate. Departments within the University also use local systems to support animal management and to monitor experimentation.

1.2 This document outlines the required management and user procedures for CCTV on the University Estate.

2 CCTV Systems

2.1 The University of Edinburgh has the following systems:

2.1.1 Estates Department Security Cameras. The Estates Department of the University of Edinburgh has in place a series of static CCTV systems. (Located as follows: Central Area, Kings Buildings, Edinburgh BioQuarter, Easter Bush, Western General Hospital, Peffermill Playing Fields)

2.1.2 Local CCTV Systems. There are a number of local CCTV systems across the University. These are used for varying tasks including enhanced security, door access control and animal welfare. A list of all systems is held in the Central security operations room.

2.1.3 Automatic Number plate Registration (ANPR) . ANPR CCTV systems are used on the Estate. These record and identify the registration number of vehicles coming onto the Estate. A list of all systems is held in the Central Security Operations room.

2.1.4 Mobile Cameras. Mobile cameras are currently not used on the estate. If procured in the future any deployment is to be considered a new installation.

2.1.5 Body Worn Cameras. The University of Edinburgh deploy Body Worn cameras (BWC) to enhance the safety and security of staff and students across the University Estate. The BWC allow the collection and collation of evidential quality video footage. Further detail on their operation is available in the separate BWC protocol.

2.2 A CCTV system consists of:

2.2.1 Camera. Mounted at selected locations. These can be fixed, manually or automatically adjustable, single or multiple lenses. Some have enhanced night and poor weather capability.

2.2.2 Viewing Platform. A monitor for viewing live or recorded feeds.

2.2.3 Data Recorders. Securely record and hold all data for a specified time period. Most also allow the secure transmission of data to viewing platforms.

2.2.4 Network. Encrypted, University owned fibre optic cable which connect the system together. (Short sections in older areas use analogue wire cables – these are less secure.)

2.2.5 Data Files. These are specified files downloaded from the data recorders. Access to these files is controlled and can be audited.

2.2.6 Management Computer. A computer designated to manage all the data files and other elements of the system.

2.2.7 Incident Management System. This is a separate system which links the data file to incidents. (Security – Perspective, Community Support – Tracker.)

2.3 For each system a comprehensive audit of all items, their location and passwords is to be in place. A copy is to be sent to the Security Operations room and the asset register updated. This should be reviewed quarterly

2.4 The following Authorised Staff are required to support a system:

2.4.1 System Manager. Responsible for the overall management of the system. Ensures this protocol and the CCTV Policy is adhered to.
2.4.2 System Operator - Download Manager. Trained and authorised to download material
2.4.3 System Operator - Authorised Viewer. Are authorised to use the viewing platform.

2.5 All authorised staff must be trained in accordance with the training paragraph in this document. (Advice can be obtained from the Security Manager.) For each CCTV system a list of all authorised personnel is to be maintained. A copy is to be sent to the Security operations room. This should be reviewed quarterly.

3 Installation and Maintenance

3.1 The following must be completed when installing a new system, or part of a system:

3.1.1 Role Specific Advice. The system manager is to ensure that appropriate professional advice is taken when locating and specifying capability for cameras. For example with a security camera the reason (Threat, High value asset, Crime spots), the type and capability of camera and the coverage required would be considered. The Security Team can give professional advice.

3.1.2 Design Guidelines. The Estates Department publishes design guidelines for 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. These must be adhered to.

3.1.3 Privacy Assessment. A Data Protection Impact Assessment (DPIA) must be completed for all new cameras. As part of the DPIA areas which must not be viewed should be identified. Pixilation or dark bands should be used to protect these areas. The DPIA is to be created on the University One Trust system and final copies held by the University Data Protection Officer in line with University processes. DPIAs should be reviewed on an annual basis.

3.2 An Operational Guidance document should written for the system. This should support the function of the system, and give direction which ensures that the CCTV Policy and this protocol are met.

3.3 The installation, repair or routine maintenance of all University CCTV systems is to be carried out by a University approved contractor. A list of currently approved contractors is held in the Security Control room.

3.4 A weekly check of all CCTV systems should be carried out. This check should ensure that cameras are serviceable, display the correct date and time and that images meet the requirements of the system.

3.5 Details of any contractor or Estates personnel involved in maintenance are to be recorded on each visit. Where required maintenance and installation contractors are able to access data held on systems.

4 Signage

4.1 Signs must be displayed in the locality of all CCTV systems. This should be in line with the CCTV Policy and the Information Commissioners Code of Practice.

4.2 The current correct wordage for these signs is held in the Security Operations room.

4.3 Body Worn Cameras are to display a warning sign advising that video and audio recordings may be carried out. They are to have a light which indicates when they are in use.

5 Training

5.1 All authorised staff using University CCTV systems are to receive initial training. This must meet current Government guidelines. At a minimum the training must cover operation of the system, data protection, privacy, legal requirements, and relevant procedures and policies.

5.2 Specific training is to be conducted prior to the issue of BWCs. This should include all of the above and specific training on the warnings to be given prior to use, and where the camera can and cannot be used.

5.3 Refresher CCTV training is to be carried out annually. The System Manager is to ensure a record of trained personnel is kept.

5.4 Further training advice can be obtained from the Security Manager.

6 Privacy

6.1 CCTV systems have the potential to intrude on individual privacy.

6.2 To mitigate the potential intrusion on an individual's privacy the System Managers are to ensure that an in date Data Privacy Impact Assessment is in place for all cameras they are responsible for. This will ensure that consideration has been given to identifying and minimising the impact.

6.3 CCTV cameras are only to be installed where essential for security or other key operational functions. Careful consideration must be given to the camera field of view, and pixilation/ dark band must be used to protect private accommodation from being viewed.

6.4 All authorised staff are to be aware of:

- The University Data Protection Policy.
- The University Data Protection handbook.
- How to report a data protection breach.
- This document, the CCTV Policy and relevant supporting operational guidance for their CCTV systems.

7 Access to live data

7.1 CCTV footage may only be viewed on system viewing platforms.

7.2 Only authorised staff, or authorised visitors/ contractors have access to live or recorded CCTV footage. A log is to be kept of all authorised visitors/ contractors and the reason they require to view the CCTV footage

7.3 Viewing platforms are to be located in closely controlled areas and protected by the use of software passwords.

7.4 The Security Manager must be made aware of remote access.

8 Management of recorded data

8.1 CCTV recorded materials (Data files) may be released to:

8.1.1 Police Scotland or other official bodies with prosecuting powers, provided that the information is necessary for the prevention or detection of crime, the apprehension or prosecution of offenders, or matters of national security.

8.1.2 Internal Departments when investigating gross misconduct of staff or breach by students of the Code of Student Conduct or related regulations.

8.1.3 Unions when representing staff in serious cases.

8.1.4 Health and Safety to support investigations.

8.1.5 Records Management and the Data Protection Officer / Assistant Data Protection Officer to support Subject Access and Freedom of Information requests regarding data held on an individual or CCTV footage held by the University respectively.

8.2 Data files are not to be copied, sold or otherwise released or used for commercial purposes, or for the provision of entertainment.

8.3 The University Security Manager or their appointed deputy must be made aware of all information release. The person making the release must ensure that the disclosure is recorded and signed for. For release of data to the Police, or other external agencies, a Data Protection Assessment must be completed. This is available from the Security Operations room.

8.4 When releasing recoded data the system will provide a date and time stamp. Any irrelevant area should be blurred or removed using the system software. The data should be recorded on a CD or DVD clearly marked, serial numbered, signed and recorded on the data release spreadsheet. This information is to be held on Perspective in the Security operations room.

8.5 Emergency release is possible, but only after consultation with the Security Manager. An Emergency Data Protection Assessment must be completed. (This is available from the Security operations room.)

8.6 The unauthorised release or misuse of recorded data would constitute gross misconduct and be subject to relevant HR disciplinary action. It may also constitute a criminal offence.

9 Retention and Disposal of data.

9.1 The CCTV system Data Recorders should be set up to hold footage for a maximum period of 30 days.

9.2 There is a time limit for the retention of downloaded footage (Data Files) as follows:

- Data Files required by Police Scotland or other official body – 12 months from the date of downloading.
- Data Files required for security internal use only – 31 days from the date of downloading.
- Printed screenshot identifying individuals – 14 days from date of printing.

9.3 If an incident is recorded that could give rise to a legal claim against the University this should be brought to the attention of the System Manager and Legal Services. Associated data files should be kept for a period of 6 years from the date of recording.

9.4 During retention all data Files and associated documentation is classed as confidential and is to be retained under secure conditions. Access to the material is to be restricted to authorised personnel only.

9.5 Following instances where footage is no longer required, or the retention periods listed above are met, the Data File is to be destroyed. (The CD or DVD is to be commercially destroyed using a University approved commercial waste company. Details of the current approved company can be obtained from the Security Operations room. A destruction certificate should be obtained.)

9.6 Images recorded on a BWC are retained for a maximum period of 30 days following recording. BWC images attached to an Incident are to be retained for periods as detailed above.

9.7 Data recorded on ANPR should be retained for a maximum of 30 days.

10 Retention and Disposal of Equipment

10.1 Hard drives on redundant Data Recorders or Management Computers are to be treated as classified waste and destroyed commercially. Details of the current approved company can be obtained from the Security Operations room. A destruction certificate should be obtained.

11 Complaints

11.1 The initial contact point for anyone wishing to enquire or complain about the CCTV system is the Security Manager. Local System Managers may be required to address any complaints about the systems they are responsible for.

12 Review.

12.1 The requirement for the continued use of all CCTV systems will be reviewed every 5 years by the Director of Estates working with the Security Manager and University Data Protection Officer.