Body Worn Video Camera (BWC) Protocol 2021

1. Introduction

1.1 The University of Edinburgh deploys 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.

1.2 The cameras are carried, and then only switched on as required. (They do not routinely record.) This document outlines the management and user procedures that must be in place for the carriage and usage of BWC.

1.3 This document should be read in consultation with the CCTV Policy and CCTV Protocol. The latter gives further direction regarding data management.

2. BWC System

2.1 The BWC system consists of:

- 2.1.1 Camera. Carried by the individual with no data storage that is user accessible. There is an indicator light which clearly indicates when the device is recording. Supporting ancillaries allow the camera to be both secure and visible when carried.
- 2.1.2 Docking Station. Supports the charging of, and data collection from the camera. It holds no data.
- 2.1.3 System Management Computer. This manages the issue of BWC, the data recorded by the cameras, and the subsequent Data Files produced. It is stand alone. (It is planned to upgrade the system onto University Servers, with password protection.)
- 2.1.4 Perspective. The Perspective incident management system is used to record all occasions when the camera is switched on, and links the subsequent data files to incidents.
- 2.1.5 Data Files. Each data file has a unique identification number. The file cannot be deleted or tampered with.
- 2.1.6 Authorised Manager. Responsible for the management of equipment issue and data download, (if applicable.)

3. Privacy

3.1 BWC have the potential to intrude on privacy. To protect privacy:

- 3.1.1 The Security Manager is to ensure that an in date Data Privacy Impact Assessment is in place for the University Estate including residential accommodation.
- 3.1.2 BWC are only to be activated when absolutely necessary and in line with the activation/guidance paragraph.
- 3.1.3 The System Security procedures are to be adhered to.
- 3.1.4 Within residential buildings carriage can only be authorised by the Director of Property and Residential Services (ACE), and then may only be used in communal areas. They must not be activated in private areas such as bathrooms or bedrooms.

4. System Security

4.1 The issue and file management system is to be password protected. The system may only be accessed by authorised managers. A list of authorised managers who can access the system is to be held in the Security Operations Room.

4.2 Data files are only to be removed from the data management computers by authorised managers following the procedure outlined in the operational guidance document. These files must be supported by the relevant data release documentation.

4.3 BWC may only be carried on the University estate by members of the Security or Community Support team.

4.4 Any breaches of security are to be reported immediately to the Security Manager.

5. Carriage/ Activation

5.1 The BWC are utilised to enhance the safety and security of staff and students. They allow the gathering of evidential quality recordings. They are also used by staff to help deescalate difficult situations.

5.2 BWC are only to be deployed as follows:

- 5.2.1 **Central Area/ BioQuarter/ Easter Bush/ Kings Building/ Peffermill**. Routinely carried by all patrolling staff.
- 5.2.2 **ACE**. Not routinely carried within University accommodation. Written authority to carry must be obtained from Director of Property and Residential Services (ACE). The current tenancy agreements for students must also refer to the carriage of BWC.

5.3 The equipment is only to be activated in the following situations:

- 5.3.1 If the security officer perceives a threat either physically or verbally to themselves or other person.
- 5.3.2 If the security officer suspects a crime has been, is being or about to be committed
- 5.3.3 If the security officer considers that video evidence will help to prevent the escalation of an incident.

5.4 A verbal warning is to be given, when possible, before BWC are used. The format of this verbal warning is not prescribed, however it must be clear to the persons present that recording is underway.

6. Reporting and Recording

6.1 If a BWC is activated a Perspective report is to be made. (Community Support must report any activations to the Security Operations Room within 12 hours.)

7. Training

7.1 All users must receive initial training on the use and care of the equipment and on the care of the BWC equipment. This will be provided by the Security Department.

7.2 Refresher training is to be conducted on a yearly basis.

7.3 The Security Manager is to ensure records of training are kept.

8. Procurement.

8.1 Security and maintenance contracts for BWC may only be procured by the Security team.

9. User Guidance

9.1 An Operational Guidance document is to be in place for the Security and for the Community Support team. This is to include managerial considerations, issue procedure, usage procedure, data download procedure, data storage procedure and release to Police and other agency guidance. This is in line with the CCTV Policy and Protocol.

10. Complaints

10.1 The contact point for anyone wishing to enquire or complain about the BWC system is the Security Manager.