



**Body Worn Cameras
Protocols & Guidelines**

General

Body Worn Cameras (BWCs) are miniaturized video cameras and microphones which capture a user's interactions with other individuals and they are usually attached to a user's clothing. Within the University BWCs are used and managed by the Estates Office Security Services Section.

The intention of this document is to provide guidance on the University's protocols with regard to the use of these devices. The document is provided primarily for reference purposes for both University staff and contractors using the cameras and when processing the data which they capture. It is also provided as a general information document for members of the public on the use of BWCs by the University.

Scope

The protocols in regard to BWCs contained in this document apply to all users of such equipment on University campuses. The primary users will be university security staff and contractors involved in the capture or processing of the data obtained.

Objectives

BWC's will be used on a range of operations across the various campuses. Their use is designed to:

- Raise standards during confrontational incidents;
- Reduce incident escalation;
- Augment opportunities for evidence capture;
- Reduce complaints;
- Assist with disciplinary and/or legal proceedings.

General Principles

- A) All Security Staff will receive the relevant training to ensure that they use BWCs in accordance with the University's CCTV & Data Protection Policies.
- B) Managers and Supervisors will be responsible for ensuring that all Security Officers using BWCs do so in a manner that is associated to the duties undertaken or at the discretion of each Security Officer after having carried out a risk assessment at any incident or location whilst on duty.
- C) BWC's will be issued to Security Staff when working in areas where confrontational incidents are likely to occur where there is a risk of threats or violence.
- D) All data captured by BWCs is 'personal data' as defined by the Data Protection Acts of 1988 & 2003 and the processing of personal data will be in accordance with the legislation. The University is the

designated Data Controller, as defined by the legislation, for all data captured or processed using BWCs.

- E) The Estates Office Security Services Section accepts primary responsibility for ensuring there is no breach of security and that the protocols set out in this document are complied with. It also has day-to-day responsibility for the management of BWC equipment.
- F) Any breach of these protocols or any aspect of confidentiality or security will be dealt with in accordance with established University disciplinary procedures.
- G) Copyright and ownership of all material recorded by virtue of BWCs in use on the campus will remain with the University.

Protocols for using BWCs

- 1) BWCs will be operated in accordance with the protocols set out in this document.
- 2) Each user of BWCs will be issued with a copy of this document. They will be fully aware of its contents, which may be updated from time to time, and he/she will be expected to comply with the protocols at all times.
- 3) Having received the relevant training in the use of a BWC, all Security Staff must ensure that the use of the camera is widely advertised prior to the start of recording to ensure fair processing. The Security Officer must be wearing **“The Video Recording in Progress Badge”** before he/she turns on the unit.
- 4) When a Security Officer decides he/she is about to record an incident, he/she must consult the Control Centre and inform the Controller that he/she is about to record an incident. The Controller must log the details on the Duty Log Book.
- 5) At the start of the recording the Security Officer must make a verbal announcement to indicate why the recording has been activated. The Security Officer should also, where possible, state the date, time, location and the nature of incident so that individuals being recorded know that the BWC is active.
- 6) The BWC must not be used in a covert manner under any circumstances. It is essential that individuals know a recording is taking place.
- 7) In general BWCs should not be used private dwellings or apartments. However in exceptional circumstances the user may, with permission from a Supervisor, use a BWC in such locations. The extent to which BWCs are used in these situations will be limited to only what is necessary for the requirements of the individual case being recorded.
- 8) The decision to record remains with the user.
- 9) Incidents that normally require reporting should be captured on the BWC.

Protocols for Recorded Data

- 1) All recorded data will be handled in accordance with the Estates office CCTV Data Protection Guidelines.
- 2) All recorded data (including downloads to portable media and prints) will be handled with care and in a confidential manner.

For the purposes of this document 'recorded data' means any material recorded by, or as a result of using, BWCs. It also specifically includes images recorded on hard drive and by way of copying to portable media including video prints.

Every hard disk image, recorded CD etc. used in conjunction with BWCs has the potential of containing recorded material.

- 3) Recorded data will not be copied, sold or used for commercial purposes or the provision of entertainment.
- 4) Unauthorised access by staff to data recorded on BWCs is prohibited and users should enforce this requirement at all times and with due care.
- 5) BWCs will be stored in a secure location within the Security Office when not in use.

Access to Recorded Material

Every request for the release of personal data generated by BWCs will be channelled through the Security Services Superintendent.

The showing of recorded material to members of the public will take place only in accordance with the law and with authorisation of the Security Services Superintendent.

Recorded material will only be disclosed to:

- a) An individual on receipt of a written Subject Access Request and once they have been identified as the person shown on the images or;
- b) To the Gardaí upon request and proper identification or;
- c) To Estates Office Management.

Members of the Gardaí (or other law enforcement agencies) have a statutory authority to investigate and/or prosecute offences and recorded material may have to be disclosed to them on a specific written request. They may also release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Any Gardaí request should be referred to the Security Services Superintendent.

Recorded material should under no circumstances leave the campus unless when being handed over to law enforcement agencies on written request or to a data subject on foot of a written 'Subject Access Request'.

Retention

Recorded material will be retained for up to 28 days after date of recording.

Each set of copied recorded material written to portable media will have a unique tracking sheet, which will be retained for at least three years after the data has been destroyed. The tracking sheet will be retained by the Security Services Superintendent.

Video Prints


A video print is a copy of an image or images, which already exist on a BWC or on a hard drive. Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken (e.g. as part of an individual Subject Access Request/legitimate Gardaí request, internal investigation of suspected criminal activity etc.)

Video prints contain data and will therefore only be released once approval is given by the Security Services Superintendent. All prints that are produced will be recorded and notified to the Security Services Superintendent who will maintain a record of such prints.

Monitoring & Audit

The Estates Office has day-to-day responsibility for the monitoring operation.

The Security Services Superintendent will be responsible for regularly auditing the operation of BWCs and for compliance with these Guidelines. Audits, (which may be in the form of irregular spot checks) will include examination of the BWC equipment and the content of recorded images.

Document Name	Body Worn Cameras Protocols & Guidelines	
Version Reference	1.0	
Document Owner	Estates Office	
Approved by	Director of Estates	
Date	January 2015	