Standard Operating Procedure (SOP)

BODY WORN VIDEO CAMERA (BWVC) PROCEDURE

SETTING University Hospitals Bristol & Weston NHS Trust

FOR STAFF Security Department

ISSUE The Trust security officer's main function is to provide a safe and secure environment that supports positive patient outcomes. Technology can significantly help improve the efficiency and effectiveness of the secure landscape. Technology does not replace officers but can and will improve the capability to achieve tangible results. Body worn video enhances contemporaneous evidence that has been shown to result in swifter justice, a decrease in spurious or malicious claims and focuses attention on the needs of the victims. Most importantly, it supports transparency and the duty of candour, therefore improves confidence and trust in the service provided.

Standard Operating Procedure (SOP)

1. Introduction

1.1 The Trust places the health, safety and welfare of its staff, patients and visitors as one of its core priorities and aims to ensure it maintains a safe and secure environment throughout the organisation. One of the ways this is achieved is by the provision of an in-house security team of officers. The security officers are highly trained professionals whose work is recognised by the retention of the National Security Inspectorate Gold Guarding scheme.

1.2 The procedure sets out the actions that must be followed by security officers operating body worn video (BWV) cameras. The provision of BWV for security officers complies with the license the Trust holds with the Information Commissioner's Office, registration number Z7060284, which allows the Trust to process information on individuals captured by CCTV images.

1.3 BWV cameras deployed by the Trust are fixed to the uniform of the officers and are capable of capturing both video and audio data. Nationally Reveal BWV cameras are used in over 50 NHS Trusts, and locally Avon and Somerset Constabulary fully deploy Reveal BWV.

2. Purpose

2.1 The security department have a responsibility to maintain a safe and secure environment, to protect staff, patients and visitors and their property, and prevent, detect and investigate security incidents. This involves interactions with staff, patients and visitors that can result in different interpretations and disagreements of events. Equally it may result in evidence not being accepted for potential criminal prosecutions. The introduction of BWV allows for the exact recording of an event in an unbiased format, where both visual and audio versions are recorded.

2.2 BWV must be seen as being complementary to the existing use of security notebooks

and Datix incidents reports, and not a replacement. BWV offers the public and the Trust better quality and more robust evidence and can work to make the Security more efficient through behaviour modifications in the presence of BWV, fewer assaults on officers and a reduction in the use of force.

3. Principles

3.1 The Security department will follow the spirit of the seven BWV principles laid down by the Home Office and College of Policing. These are:

3.1.1 The use of BWV is lawful

3.1.2 Data will be processed and managed in line with the principles of the Data Protection Act

3.1.3 BWV use will be overt

3.1.4 Operational use of BWV must be proportionate, legitimate and necessary

3.1.5 Use of BWV will be incident specific, officers are required to justify their use or non-use of BWV

3.1.6 BWV does not replace conventional forms of evidence gathering, it supports them

3.1.7 Consultation with local parties with regard to deployment

3.1.8 Therefore; the use of BWV will be:

- Proportionate
- Legitimate
- Necessary
- Justifiable

4. Responsibilities and Roles

4.1 Head of Security (HoS) and Security Manager (SM)

The HoS or SM will be responsible for the auditing of this procedure to maintain compliance with the above seven principles and the associated legal compliance; the General Data Protection Regulation, Data Protection Act 2018, Human Rights Act 1998 and European Convention on Human Rights. The SM will ensure security officers have received required training in the operational use of the BWV including section three above.

The HoS or SM will provide assurance to the Trust Risk Management Committee, the Trust Health, Safety and Fire Committee and at Divisional level the Estates and Facilities Risk Management Group in the form of reports, incident summaries and/or periodic reviews.

4.2 Security Officers

4.2.1 No security officer will be deployed with a BWV camera unless they are trained and can demonstrate their responsibilities and duties in BWV operation on Trust premises. Training will include practical use of equipment, operational guidance and the BWV principles, when to commence and cease recording and the legal implications of the use BWV. On completion of BWV training the security officer will sign a compliance certificate. Failure to comply with the BWV procedure or the BWV principles could result in a Disciplinary Investigation being undertaken.

4.2.2 BWV will be issued at the commencement of duties and assigned to individual officers. The officer will ensure the BWV is operational (image and audio quality), date and time is correct and fully charged. The BWV will be fixed to the officer's stab vest and will be worn on attendance to all incidents.

4.2.3 BWV MUST NOT be activated for normal patrolling of Trust premises. BWV will also

not be used by the Trust to performance manage their employees. Security officers are to advise HoS/SM of all requests to do so.

4.2.4 On attending an incident where BWV is required ALL attending security officers MUST ACTIVATE their individual units. The scope of when to activate and when not to activate is a matter of judgement for security officers with the one exception:

4.2.4.1 Security officers MUST activate their individual body cams in ALL incidents where any type of restraint is deployed - physical or mechanical. Activation MUST take place regardless of the reason of the need for restraint being undertaken, clinical or non-clinical. There are NO EXCEPTIONS to these instructions.

4.2.4.2 The purpose for all restraint to be recorded is to fulfil the Trust Safeguarding obligations to our patients and stakeholders. It allows vital evidence to be gathered, including post incident location of objects, instructions given or to record incident details in a fluid event.

4.2.4.3 Failure to activate BWV by security officers on attending an incident will require written justification from the security officer. In the circumstances where restraint is used and BWV is NOT activated, a Disciplinary Investigation could be activated to check if actions were appropriate.

4.2.5 Wherever possible recording will not commence until the officer has issued a verbal warning of their intention to turn on the BWV. This should include the date, time and location together with a confirmation that the incident is being recorded using video and audio. At the end of the incident the officers should make a verbal announcement that the recording is being stopped before stopping the recording.

4.2.6 BWV may be used to capture the first account of an incident from those affected or witnesses but only when there are time limitations. Permission must be obtained prior to commencing recording and a full explanation given for the recording to those providing the account. However, it must not be used to generally record statements or reports from victims and witnesses, especially if there are no time constraints and the police are attending the incident. No interviews under caution can be conducted by security officers.

4.2.7 Before completion of duty the BWV user will transfer all recorded data from the camera to Digital Evidence Management System (DEMS) for secure storage and retention. There are no circumstances in which the unauthorised deletion by the user or other persons of any data can be justified. Any evidence that data or BWV unit has been tampered with or attempted may result in legal and/or disciplinary proceedings.

4.2.8 The security department will hold all BWV recordings. Access to the recording will be restricted to authorised personnel within the security department and law enforcement agencies via DEMS. Any recording that requires retention for evidence in potential court proceedings will be recorded as evidence in DEMS and retained in line with current legislation. Non-evidential data will be retained for 90 days before being automatically deleted by DEMS. The 90 day period will allow for investigations and complaints to have access to BWV data.

4.2.9 At the end of a shift the officer is responsible for making sure that the BWV unit is in good working order and suitable for the next officer. Any damage or malfunction must be reported to the HoS and/or SM. Care should be taken to ensure that the device and any batteries are placed on charge correctly.

5. Objections to Recording

5.1 In principle, security officers are not required to obtain the expressed consent of the person or persons being recorded by their BWV unit. There should always be a tendency to record, within a legal framework, unless circumstances dictate otherwise. An officer who fails to record an incident will be required to justify their actions especially if their colleagues continue to record, or vice versa.

5.2 If the subject/s of an incident requests that the BWV be switched off, the officer should advise the person/s that:

- Any non-evidential material is retained for a maximum of 90 days only and then automatically deleted
- That the data is restricted and will not be disclosed to third parties unless relating to criminal matters
- That the subject's data can be accessed on request via a subject access request in accordance with the GDPR

6. Collateral Intrusion

6.1 In so far as is practicable, officers should restrict recording to areas and persons necessary in order to obtain evidence and intelligence relevant to the incident and should attempt to minimise collateral intrusion to those not involved.

7. Professional Conduct

7.1 Complaints about the conduct of security officers should follow normal Trust procedures. BWV material is usually obtained and retained during an incident where security officers have either come across potentially criminal behaviour or called to support Trust staff deal with an aggressive patient or visitor. However, officers must be aware that captured data can be used to investigate a complaint made against them.

7.2 BWV may contribute to a net reduction in complaints and the commencement of disciplinary action by providing a clear and impartial record of the interaction. This means that when a complaint is made the data can be used quickly to establish what happened and provide a speedy resolution.

7.3 BWV data that is relevant to an investigation of a complaint should be secured, reviewed and retained at the earliest opportunity.

8. Data Audit Trail

8.1 The use of BWV devices can generate a large amount of data that must be stored appropriately and retained, reviewed and deleted. To provide authenticity of recordings in the event of a criminal trial evidential continuity statements may be necessary and should include the following:

- equipment serial number/identifying mark
- day, date and time the user took possession of the unit (A)
- day, date, time and location recording commenced (B)
- day, date, time and location recording concluded (C)
- day, date, time and location that the master copy was created and retained securely (D)
- if any other person had access to or used the unit between A, B or C and time D an additional statement will be required from that person

8.2 Where more than one BWV unit is present at the scene of an incident or the area is covered by CCTV, then all data should be secured and retained to allow a full perspective of the incident to be available to law enforcement agencies or other effected parties. Failure to secure all available data may result in legal or disciplinary action if deemed to be tampering with evidence.

9. BWV as a Post-event reflection aid

9.1 To aid post-event reflection and learning the Trust retains the right to use BWV data to review and enhance how incidents are dealt with, improving professionalism of security officers and providing a powerful tool for behaviour change and continuous improvement. Such data will be strictly restricted, reviewed by Safeguarding and deleted within 28 days unless required for criminal or Safeguarding investigations.

10. Legislation

10.1 General Data Protection Regulation (GDPR) - The GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). The main provisions of both these apply from 25 May 2018. The GDPR applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

10.1.1 The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Personal data is information that relates to an identified or identifiable individual.

10.1.2 The GDPR sets out seven key principles which lie at the heart of our approach to processing personal data:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

10.2 Data Protection Act 2018 (DPA) – The DPA, by applying the GDPR, regulates the processing of personal data or sensitive personal data, whether processed on computer, CCTV, stills camera or any other media. Any recorded image that captures an identifiable individual is covered by the DPA. Officers should be aware that people captured in a BWV recording are entitled to obtain a copy via a subject access request to the HoS or SM, be able to explain how to obtain a copy and know the retention and deletion criteria of captured data.

10.3 The European Convection on Human Rights – Article 6 of the ECHR provides for the right to a fair trial. All images from BWV can be used in any potential court proceedings whether they provide information that is beneficial to the prosecution or the defence. Article 8 of the ECHR is the right to respect for private and family life, home and correspondence. Therefore the use of BWV must be used in accordance with the law and proportionate. In principle the use of BWV is justifiable for the preventing and detecting of crime, even in a clinical setting.

10.4 Freedom of Information Act 2000 – FOIA grants a general right of access to all types of recorded information held by public authorities, which may include digital images recorded by BWV. However as they contain personal data BWV images will be typically exempt from FOIA disclosure unless fully anonymised. All FOI requests made directly to security officers or the LSMS/SM should be directed to the Trust FOI procedure.

10.5 Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice – Part 2 of the PFA deals with regulation of CCTV and other surveillance camera technology and introduces the Surveillance Camera Code of Practice. However, NHS organisations are not included as relevant authorities and therefore do not have a duty with regard to the code.

Table A

REFERENCES	General Data Protection Regulation Data Protection Act Human Rights Act Freedom of Information Act Protection of Freedoms Act
RELATED DOCUMENTS AND PAGES	Security Policy
AUTHORISING BODY	Estates & Facilities Risk Management Group
SAFETY	
QUERIES AND CONTACT	Security Management Team Ext. [redacted]

Appendix 1 – Sign off process

Once your document has been written, it should go to the relevant group for approval. This might include the Steering Group for the relevant speciality, or the Governance Group for the relevant division, especially if the document covers many different specialities/departments.

If you are unsure of who your document should be signed off by, please contact [redacted] where the team can advise you.

Once your document has been signed off, include the name of the authorising group in **Table A** above and send the document to [redacted] for uploading. Please note: this can take up to **two weeks** to be completed.