

Contents

1.	Scope	2
2.	Procedure	2
3.	Definitions	8
4.	Responsibilities	8
5.	Audit and Review (evaluating effectiveness)	8
6.	References	8
7.	Financial Checkpoint	9
8.	Equality Analysis	9

1. Scope

- 1.1. South East Coast Ambulance Service NHS Foundation Trust (the Trust) is committed to the safety and security of our work colleagues. This procedure sets out the operational arrangements for the deployment of Body Worn Video (BWV) as part of an ongoing trial.
- 1.2. The Trust is committed to deterring those who may be minded to violent and aggressive behaviour towards our colleagues and wherever possible, and where this has occurred, to seek the strongest forms of sanction and redress available. Therefore, the Trust has approved the use of BWV as part of an ongoing trial to support the criminal justice system and to bring perpetrators to justice.
- 1.3. This procedure is applicable to all Trust BWV users and sets out the scope of practice to which our BWV users must adhere.

2. Procedure

2.1 The Key Principles of Body Worn Video (BWV):

There are certain principles for the use of overt BWV which reflect the strategic underpinning of Trust policy and procedure.

BWV is being trialled to assess its impact in helping to reduce violence and abuse of SECAmb colleagues while carrying out their duties and will contribute to the Trust's Violence and abuse Reduction Programme.

2.2 Training:

All BWV users must be appropriately trained, signed off, and have access to BWV equipment.

Users of BWV will be required to receive a training package and be given additional guidance on its use prior to initial operation.

During out of hours, support for BWV will be provided by Critical Systems as per published on call report.

During office hours support for BWV will be provided at a local level by Make Ready Centre Managers (MRCM) and the Security Department.

As well as being familiar with this Procedure and the related BWV Policy, users will also be required to ensure that they are familiar with the Information Governance Policy, the Data Protection Policy and Data Subject Access Request Policy. They will also need to have been completed during their annual statutory and mandatory IG training.

Once a user has completed the practical training, familiarised themselves with the procedure and policies, and signed training competencies they will be authorised to use the BWV device, and an account will be activated.

Training content, delivery of training and recording of training records for BWV users will be coordinated by the Head of IT and Health, Safety and Security.

2.3 Equipment:

The BWV equipment is a body-mounted camera with an in-built microphone. The BWV stores digital files which, once recorded, can only be viewed, deleted, or amended by the following authorised personnel:

- Head of Health, Safety and Security
- Security Manager
- Head of IT
- Security Team or Critical System team

Each digital file carries a unique identifier and is time and date stamped throughout.

Dedicated software will manage the downloading, storage, exporting of files and/or burning to DVD of the digital files for evidential purposes. This provides a full audit trail.

It is the responsibility of the Head of IT to keep an asset register of the serial numbers and location of each BWV within the Trust.

It is the responsibility of each individual BWV user to report any malfunction immediately via the Trust incident reporting system (Datix). The Security Team will liaise with the supplier as necessary for the return of faulty BWV equipment.

Any misuse of BWV must be reported via the Trust incident reporting system (Datix) and brought to the attention of the Head of Health, Safety and Security and Security Team who will liaise with other relevant departments to investigate the matter (e.g. Human Resources). Misuse of the system may result in action taken which will be in line with the Trust's Disciplinary Policy and Procedure.

Any unresolved software issues will be reported to the system supplier by the Security Team.

2.4 Issuing of BWV Equipment:

Only users who have received the appropriate training are authorised to use the equipment. BWV will be available to be booked out at the start of each shift, using the following process:

The operator will use their issued Trust ID card to take out a BWV by tapping the card onto the card reader. The BWV system will then provide a visual and audible indication to identify the specific BWV allocated.

The BWV can then be removed from the docking station for use.

Users must connect their BWV to the docking station on conclusion of their shift and must not hand-over to another user without completing the proper booking out procedure, even if no footage has been recorded. This is the user's responsibility and must be adhered to. Users should not commence shift with a recording device that contains data of incidents from a previous shift, or a device that is not charged.

2.5 Returning Equipment:

Users must return the BWV to a docking station prior to their shift end. Users must check the BWV is securely docked to ensure that the battery will be re-charged.

If the BWV has become damaged, or a fault is identified, the user must complete a Datix incident report as soon as practically possible, and in any case prior to end of their shift, so that the Security Team is notified.

BWV should be cleaned at the end of each shift following the system detailed in Action Card (1) BWV Decontamination.

2.6 Faulty Devices:

Any faulty equipment must be checked firstly by the MRCM and then backloaded to the Security Team where a fault has been confirmed. BWV equipment should not be disposed of by any other means.

2.7 Loss of a Device:

If a BWV is lost or stolen, or it is suspected that a data loss has occurred, this must be reported as soon as the loss or theft is discovered on Datix DIF (1). Devices will have a label with Trust name "South East Coast Ambulance Service and logo.

2.8 The recording process:

The decision to record or not to record any incident of violence and abuse always remains at the discretion of the trained user. The sole purpose of recording is to capture evidence relating to an incident of violence or abuse. A BWV is not to be used for any other reason.

BWVs are being made available to staff to help reduce the impact of any incident of violence or abuse and are to be activated when the wearer feels at risk of violence and/or abuse or when a situation escalates or is at risk of escalating and the wearer feels vulnerable or at risk.

However, users must be mindful that failing to record an incident of violence or abuse, which would have been of a significant nature, may require further explanation at any subsequent internal or external investigations/audits to understand the reasons why.

BWV trained staff who are wearing BWV should activate their device when their risk assessment of the situation indicates an increased potential threat to the safety of the user and/or their colleagues or members of the public.

If a BWV is intentionally activated this must be recorded on the Patient Care Record (PCR), where applicable and a Datix incident report raised even if the incident deescalated and nothing untoward occurred.

A recording indicator (a red light) is visible when recording is activated. Staff should, wherever possible (based on a risk assessment at the time), tell people that they are recording video and audio for crime prevention before activation and immediately after activation. The device will have signage to indicate that images/audio may be recorded, shown in mandatory warning signage format (yellow and black).

Unless specific circumstances dictate otherwise, it is a legal requirement under the Data Protection Legislation, UK GDPR and Data Protection Act 2018 to provide fair processing information where possible/practicable and announce to the subject(s) of an encounter that video and audio recording is taking place using BWV (College of Policing, 2007).

Recording must continue uninterrupted from the commencement of recording until the conclusion of the incident. BWV users must be satisfied that an incident has reached its conclusion prior to finalising any recordings.

Request for access to footage will be as per the Trust Data Subject Access Request Policy and Procedure for both clinicians, patients and other subjects captured during recording.

2.9 Recording in Sensitive Areas/Locations/Circumstances:

Users are to be cognisant when using BWV in sensitive areas, i.e., hospitals, police stations, prisons, and refuges, etc. Users should adopt a common sense approach and take particular care not to record anything which may:

- Risk the security or safety of any person, premise, or property
- Negatively affect the on-going care or treatment of any person
- Unnecessarily inflame/provoke a situation

Further justification will be required when considering activating BWV in more sensitive areas, such as: schools; care homes, etc. The pressing social need will have to be far greater for the use of BWV to be necessary and proportionate. This will require the operator to provide a higher level of justification to evidence supporting the need for its use than might otherwise be required.

2.10 Objections to Recording:

The use of BWV by the Trust is being introduced for a legitimate safety purpose and, in principle, users are not required to obtain the expressed consent of the person or persons being filmed whilst there is a perceived threat to staff safety.

The video recording will not necessarily be ceased at the request of a member of the public. It is for the user to consider whether to cease BWV recording depending on the threat to safety.

2.11 Collateral Intrusion:

BWV will have a user-controlled pre record buffer. Once active the buffer will be for a rolling 30-seconds. When recording mode is started any available buffer footage will be added to the start of the recording. Only the saved footage from the activation and any buffer prior to activation will be saved when the BWV is returned to the docking station. If a BWV is not activated during a shift and is only on standby and buffering, then when the BWV is returned to the docking station, no recording will be uploaded and any buffered footage on the BWV will be deleted automatically by the system.

Each recording should be incident specific and justifiable by the user. As far as is reasonably practicable, recordings should be restricted to areas and persons where it is necessary to obtain evidence relevant to the incident. The user should be mindful of minimising the potential for collateral intrusion.

Any persons recorded as part of an incident can, and may, be deleted/redacted from the footage by an authorised person. Users must note that this process will be carried out when the footage is required as part of an investigation. The original file that contains the footage will not be affected as the original will be kept maintaining evidential integrity. All editing will create a new file that is linked to the original.

It must be remembered by the BWV user that continuous recording will require strong justification as it is may be considered excessive and cause a great deal of collateral intrusion. This is because continuous recording is likely to capture people going about their daily business, as well as the individual who is the focus of attention.

2.12 Uploading and File Referencing:

It is the responsibility of the individual BWV user to ensure that footage can be correctly downloaded by ensuring the BWV is docked correctly at the end of shift. Users must return the device to a docking station so that recorded footage is downloaded, the BWV is cleared of all data and ready to be booked out again (once the battery has recharged). Once the BWV is plugged into the docking station, all recorded footage is automatically downloaded and is saved on the secure data storage facility and available for evidential review by the authorised persons.

2.13 Exporting Data and Producing Exhibits:

The BWV data management system is fully auditable and will identify all footage edited and / or exported from the system by any means. It is a disciplinary offence, and potentially a criminal offence, to do so for anything other than a legitimate purpose. The process for exporting footage forms part of the practical training received by authorised persons.

It is the responsibility of the authorised persons to ensure that any appropriate footage is made available in a format that is suitable to the requirements of where it is to be played. Data is only retained for 30 days although we may if appropriate and with a legal basis retain for a longer period.

All images from BWV have the potential for use in court proceedings whether they provide information that is beneficial to the prosecution or defence. The information will be safeguarded by an audit trail in the same way as other evidence that is retained for court.

The Trust has a full privacy notice, an employee privacy notice and information available on its public facing website which meets its adherence to transparency principles.

BWV Footage must only be used for the purpose of supporting evidence to criminal proceedings and for no other reason.

2.14 Private Capture Equipment:

Only devices issued by the Trust are to be used for the purpose outlined in these procedures.

2.15 Health and Safety

Violence and abuse risk assessment will include the use of BWV. Devices are lightweight, un-intrusive and present no transmission or electrical risk. However, the following areas have been identified to present potential risk and users should consider the following risks:

- Fuelling vehicles there is no identified risk in this area, there is no reason users cannot refuel their vehicles whilst wearing BWV.
- Explosive Devices BWV should not be used at the scene of suspicious packages/explosive devices.
- Hazardous Material BWV should not be used around highly flammable/explosive substances or chemicals. Advice should be sought on a case-by-case basis from the Tactical Advisor when attending COMAH sites, though the guiding principle is that BWV should not be used.
- Personal Safety There is a risk that users may be confronted by persons attempting to grab the BWV equipment. Conflict Resolution Training to disengage and remove oneself should be used.
- Snagging There is a possibility of the device catching on clothing or seatbelts etc. Users should be mindful of this when entering/alighting vehicles and in environmental situations where there is an increased risk, i.e. confined spaces.
- Improper Use Users will receive full proper training on the use of and wearing BWV equipment. Users should seek advice/support from line

management if they are unsure and until clarification occurs, users should not activate the BWV.

• Further Risks – Any user who identifies additional risk associated with the use of BWV should take appropriate steps to bring it to the attention of their line manager, other appropriate person, or the Health, Safety and Security team.

3. Definitions

BWV: The BWV is a body mounted camera with built-in microphone. The camera stores digital files which, once recorded, cannot be deleted, or amended by the user. Each digital file carries a unique identifier and is time and date stamped throughout.

Buffer: Trust BWV will have a user-controlled pre record buffer. Once active the buffer will be for a rolling 30-seconds. When recording mode is started any available buffer footage will be added to the start of the recording. The buffer period will be video only and will not include audio.

4. **Responsibilities**

Are set out in section 4 of the Trust's BWV policy.

5. Audit and Review (evaluating effectiveness)

- 5.1 All procedures have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new procedure is approved and disseminated.
- 5.2 Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).
- 5.3 This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.
- 5.4 All changes made to this procedure will go through the governance route for development and approval as set out in the Policy on Policies.

6. References

Data Protection Act 2018

Human Rights Act 1998

Freedom of Information Act 2000

Equality Act 2010

Home Office - Technical Guidance for Body Worn Video Devices - Oct 2016

The Regulation of Investigatory Powers Act 2000

7. Financial Checkpoint

This document has been confirmed by Finance to have no unbudgeted financial implications.

8. Equality Analysis

- 9.1 The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude noone. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.
- 9.2 Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.