# Body Worn Video Cameras Policy Framework Section 6 Guidance

### **CONTENTS**

Section	Title	Page
1	Current Legislation	4
2	Camera Operation	4
	2.1 Booking out a camera	4
	2.2 Point to start recording	5
	2.3 During Recording	5
	2.4 Cessation of Recording	6
	2.5 Partial recording	6
	2.6 Transcripts	6
	2.7 Dealing with objections to being filmed	7
	2.8 Staff development, Allegations, Complaints, and Investigations	8
	2.9 Post Incident procedures	8
	2.10 Scenes of Crime/Preservation of evidence	9
3	Staff Training and development	9
	3.1 Staff Training	9
	3.2 Prisoner development	10
	3.3 Legal Privilege/confidential communications	11
4	Data Management	11
	4.1 Copying/saving footage to disc or USB flash drive	11
	4.2 Disclosing footage for criminal evidential purposes	11
	4.3 Disclosing footage for Intelligence purposes	12
	4.4 Disclosing footage to the Prisons and Probation Ombudsman as part of a complaint	14
	4.5 Disclosing footage to the Prisons and Probation Ombudsman as part of a Death in Custody investigation	15
	4.6 Disclosing footage to an internal investigator as part of a Disciplinary Investigation	15
	4.7 Disclosing footage as part of an adjudication hearing	15
	4.8 Third party requests – Subject Access Requests	16
	4.9 Footage Redaction / Pixilation	16
5	Operational Scenarios	18
	5.1 Use of Body Worn Video Cameras Outside of an Establishment	18

	5.2 Spontaneous Use of Force (UoF)	18
	5.3 Planned Use of Force (UoF)	19
	5.4 Nights	19
	5.5 Incident Response – areas where visitors/members of the public are present	19
	5.6 Incident Response – Medical Intervention	20
	5.7 Routine Medical Treatments	20
	5.8 Dogs Teams & Dedicated Search Teams	20
6	System Management	21
	6.1 User – the person wearing the BWVC unit is responsible for	21
	6.2 User/View footage	21
	6.3 Administrator	21
	6.4 Approval Officer	21
	6.5 System Owner	22
	6.6 Assigning Users	22
	6.7 Equipment Management	22
	6.8 System access	23
	6.9 Documentation	23
	6.10 Justification assessment must set out the following information	23
	6.11 Justification/decision log must capture the following information	23
	6.12 Evidence log must capture the following information	23

### **BWVC Policy Framework Guidance**

### Guidance

This document provides guidance to prisons on the implementation of the BWVC Policy Framework including evidence, good practice and templates and forms part of the overall Policy Framework.

### 1 Current Legislation and guidance

The Prison Rules 1999

Data Protection Act 2018 (DPA) and UK General Data Protection Regulation

Regulation of Investigatory Powers Act 2000

Protection of Freedoms Act 2012

Freedom of Information Act 2000

Surveillance Camera Code of Practice

https://www.gov.uk/government/publications/update-to-surveillance-camera-code

### 2 Camera Operation

### 2.1 Booking out a camera

As a minimum all operational staff within band 3 – 5 within the closed estate will collect a camera from the camera docking station at the beginning of their shift. When removed from the camera docking station the camera will enter 'stand-by' mode and commence a 'pre-record' function, the footage captured by 'pre-record' will only be saved when camera recording is activated by the user.

Within the open estate, those roles designated by the Governor with the Local Security Strategy (LSS) as being required to wear a BWVC must collect a camera from the camera docking station at the beginning of their shift. When removed from the camera docking station the camera will enter 'stand-by' mode and commence a 'pre-record' function, the footage captured by 'pre-record' will only be saved when camera recording is activated by the user.

When worn, BWV cameras must be turned on and set in the standby mode. An officer can record an event immediately through touch activation of the record button. In standby mode BWVC records on a rolling buffer. When the camera is activated by the operator, video and sound recording starts and automatically includes the back-captured buffer video.

### 2.2 Point to start recording

Staff responding to an incident should serve as a prompt to users to commence recording at the earliest opportunity; to maximise the material captured by the camera. It may be helpful for establishments to include a reminder for staff to switch on BWVC at the point an Alarm is called over the radio net. For example [two tone] "General Alarm G3 landing, staff to activate Body Worn cameras, I say again, General Alarm G3 landing, staff to activate cameras immediately"

This will remind staff at the scene to switch on their cameras, potentially capturing footage of an incident as it happens. It will also prompt those staff responding to switch on their cameras enroute capturing footage of the scene and events immediately on arrival.

### 2.3 During Recording

Users must always ensure that BWVC is only used as an overt audio or overt visual recording mechanism and is not intentionally used covertly.

Upon activating their BWVC, users must make a clear verbal announcement to anyone in the vicinity that the recording of both audio and visual images is taking place. This must take place as soon as it is possible and safe to do so. If the BWVC is activated prior to arriving at the scene of an incident, then the announcement must be made to those at the scene once it is possible and safe to do so. An agreed establishment wide standard form of words covering these points can be adopted for continuity purposes. For example: for your safety and the safety of others you need to be aware that everything you say and do will be recorded.

It may be helpful, ONLY if circumstances permit and dependent on the type of the incident or event being filmed, for the user to provide verbal commentary during the incident/event. This will prove helpful when the user is unable to record elements such as smells or events occurring outside of the camera's field of vision.

Recording must, where practicable, be restricted to those individuals and areas that are necessary to record in order to obtain material relevant to the incident or event. It is important that users minimise the risk of collateral intrusion on those not involved in the incident wherever possible. However, and importantly, this must not be at the expense of failing to obtain enough coverage of the incident/event or restricting the user's movements and ability to manage the incident.

There may be occasions when recording is inadvertently stopped or disrupted during an incident or event. This is most likely to occur where a BWVC is knocked or turned off during a struggle, where there is a technical failure or where the view of the camera and/or microphone becomes obstructed or compromised for some reason. Where this occurs and the user becomes aware recording must be recommenced and a supporting explanation provided on film as soon as practicable in addition to being documented in any subsequent written statement.

Once recording has been competed the data must be retained and handled as 'official sensitive' in accordance with:

- this Policy Framework,
- PSI 2018-03 the Data Protection Act (2018), General Data Protection Rules, the Freedom of Information Act (2000), Environmental Information Regulations 2004
- PI 2018-02 Records, Information Management and Retention Policy and,
- Established procedures of the establishment as set out in the Local Security Strategy (LSS).

### 2.4 Cessation of Recording

In the same way that a user will record their decision to activate BWVC so too will the decision to cease recording be documented. In making this decision users must be satisfied that the risk of not capturing further helpful material is minimised.

Under normal circumstances users must cease recording either when:

- The incident has concluded to a safe and secure position
- It is no longer justifiable, necessary, or proportionate to continue recording

### 2.5 Partial recording

There may be circumstances where an incident is only partially recorded, for reasons such as accidental damage, technical failure, the BWVC becoming dislodged or the camera lens being inadvertently obscured. There may be other occasions when the audio recording is unclear due to high levels of surrounding noise.

In all cases users are to remain vigilant throughout the duration of the incident and gather and retain material through normal means (non-video). Users are to still complete the necessary written statements following any incident noting the reasons for the lack of BWVC material.

If users attend an incident and are recording the scene or any part of the incident/location using BWVC then the entire incident should be recorded unless there are exceptional reasons not to do so or a manager instructs them to stop filming.

### 2.6 Transcripts

In some circumstances it may be necessary to obtain a written transcript of the audio material captured on BWVC for example where: -

- The sound is of a poor quality
- The audio contains a high degree of slang
- A foreign language has been captured and a translation is considered necessary

Even when a written transcript has been provided, the accompanying visual and audio footage will contain a degree of information not captured in the written word, such as gestures, tone, and non-verbal communication which will, when considered with the written transcript, put the text into context.

Where a transcript is produced it should be treated as evidence and handled in accordance with evidence handling processes for the establishment, the accompanying footage will be retained, and a note made on the retention log cross referencing the details of the transcript.

### 2.7 Dealing with objections to being filmed

Any objection by a prisoner(s), visitor(s) or other person to the use of BWVC to record, must be addressed by the BWVC user with a clear and concise explanation why recording is taking place. The user must explain to the prisoner(s)/visitor(s) the benefits of recording the encounter; which may include explaining that the recording is to safeguard all parties by ensuring an accurate reflection of any action or comments made by either party. Users may also direct visitors to the signage which explains that BWVC/CCTV is used in the establishment and in the case of a complaint to write to the Governor.

The user may also explain that non-evidential material is only retained for a maximum period of 90 days and that any access to the material is both limited and controlled; BWVC material is restricted and any disclosure of personal information in relation to living young persons, young adults and adult offenders must not be disclosed even to close relatives without the offender's consent. In the event of disclosure to third parties, (such as the police or courts, this would be in line with the Data Protection Act 2018 (DPA). Further guidance can be found in Information Requests Policy Framework.

If the prisoner or visitor continues to object, then the user must decide based on the circumstances of the incident or event. Stopping filming at the request of a prisoner would however be an exceptional occurrence and the normal policy would be to continue to film and to record the prisoner's objections on film and within the accompanying written document.

An example of such an objection may be where filming captures a prisoner's intimate body parts. Whilst it may not be appropriate to film a prisoner's intimate body part, there may be occasions where a prisoner is either in a sensitive area such as the showers or is partially clothed, but their behaviour is violent and aggressive and where the over-riding requirement is to record what took place. Such circumstances will be exceptional, and, in each case, the accompanying paperwork must set out the justification for recording such images.

Where such footage contains intimate body parts, consideration must be given to pixilation of the footage where there is a need for copies to be made or for it to be made available for viewing as part of an adjudication. It is important that the master copy remains "un-changed" on the system. Please consult the redaction / pixilation section (section 5.10) of this guidance for further information.

There may also be occasions when continued recording is exacerbating the situation and is hampering de-escalation of the incident and possibly increasing the likelihood of a violent confrontation. In such circumstances it is for the user to make a judgement based on the facts and view at that time and where able the user should state the intention to stop recording together with a brief explanation.

If at any time the user considers it inappropriate to continue to record specific events the user could take the decision to end recording and in doing so explain verbally before the recording is stopped. The user must then also record the rationale for the decision in the accompanying paperwork/report.

Equally users may be approached by a prisoner or other person with a request to film an encounter or particular situation. It is for the User to decide if this is appropriate and consider the reasons for the prisoner's request, however there should be a presumption in favour of doing so. The user's decision will be explained to the prisoner. If they do refuse to switch the camera on, then BWVC users must log the refused request using the system in place at the individual establishment and submit an Intelligence Report.

### 2.8 Staff development, Allegations, Complaints, and Investigations

BWVC footage can be used to quickly resolve complaints and avoid lengthy investigations as well as highlighting good work done by users and positive responses from prisoners.

All allegations and complaints received from prisoners, staff or visitors regarding the conduct of others must be dealt with in accordance with the establishment's own procedures.

BWVC users must inform the appropriate manager investigating a complaint of the presence of BWVC material at an early stage so that a decision can be made whether the footage should be tagged and how any material will be used.

Any investigating member of staff will, with the authority of the Investigation Commissioning Officer, be able to review the BWVC material where available for a period of up to 90 days after recording. If the incident has been tagged for retention, such as if the incident involved Use of Force, then it may be viewed beyond this 90-day period. The investigating member of staff must consider the requirements of PSI 2010-06 — Conduct and discipline, in respect of the requirements to disclose relevant BWVC material to the member of staff under investigation.

BWVC material may be shown to the complainant and noted in the relevant record. However, only the specific material relating to the incident/complaint subject matter must be reviewed and consideration must be given to obscuring/redacting images of non-connected person(s) and the decision to obscure/redact or not disclose should be recorded.

BWVC material must be retained on the system and marked as required for an investigation/complaint until it is confirmed that all potential uses of it, including appeal mechanisms have been completed.

### 2.9 Post Incident procedures

Post incident procedures may include a number of routine working practices such as cell clearance, where the occupant was involved in an incident and has subsequently been relocated. Whilst BWVC must not be used to record routine working practices, in the direct aftermath of an incident it may be appropriate to record such procedures. Such recordings must only be made on the clear instruction of the Incident Manager and factors requiring this clearly set out in the accompanying written statements.

When dealing with incidents involving Potential Traumatic Events (PTE) (which is defined as an event that may cause acute stress reactions afterwards.) Incident Managers and supervisors may consider the potential effect reviewing those involved in the incident reviewing captured footage and the possible impact of re-traumatisation. It is not possible to identify here every scenario which has the potential to give rise to post trauma stress reactions in all cases, as such reactions are very personal and individual. Incident Managers can refer to Post Incident Care Policy Framework for further information and guidance on this.

### 2.10 Scenes of Crime/Preservation of evidence

Prison staff must focus on direct management of the incident at hand and not assume any of the investigatory role which remains to be the role of the police.

In responding to incidents users may arrive at a potential "crime scene" and footage captured may prove useful for any subsequent police investigation. It is important when capturing a "crime scene" the user does not interfere, move or change any element therein, in line with the requirements of PSI 2016-08 - Dealing with evidence and the Crime in Prison Referral Agreement.

With incidents it is important that in line with established incident management procedures the scene is secured (regardless of BWVC footage) until the police have attended and released the scene. This will be the case for deaths in custody, serious assaults and other serious incidents.

It is extremely important that all staff understand that it may harm a police investigation or prosecution if BWVC is used to pursue lines of investigation where statements are obtained in the absence of a caution particularly where the suspected perpetrator is interviewed. Audio and visual recording of suspect interviews may be completed in certain limited circumstances, to be considered by officer in charge of the investigation, however staff should limit the initial questioning to:

Identify if an offence has been committed

 Identify and mitigate against any ongoing or further risks – manage the incident and those involved

Establishments must set out in their local contingency plans the necessity to secure all digital footage, which can be achieved by prompt uploading of the footage to the networked solution.

### 3 Staff Training and development

### 3.1 Staff Training

When BWVC footage is being considered for use in training, staff must first consider whether any alternative methods would serve the same purpose, other than using BWVC footage.

HMPPS could suffer reputational damage whenever personal information is being used or shared incorrectly. Their also considerations of the use incident footage which may create PTE or acute stress reactions in those who view the footage. If no alternative is viable or appropriate, then BWVC footage can be used, subject to the requirements below and the requirements in the policy framework would apply to its use. But this must be considered on a case-by-case basis.

The following are points of consideration:

- Is anyone in the footage identifiable (also from anyone's knowledge of the incident)? If so, the footage should be pixelated
- What is the setting of the incident recorded and is it contentious (such as toilets, showers or places of worship)? This would point against using the footage for training purposes.
- Is the footage being used informally in a debrief setting, or is the footage going to be used as part of a larger/more formal training event? Use of footage for training and de-briefs should be carefully considered to ensure that only the minimum detail necessary is included. This is even more significant if the footage is going to be shown to many people or retained for a long time.

Showing footage for training which is highly emotive, challenging or distressing has the potential to cause harm to both prisoners, staff and in some circumstances prisoner's family members. Governors must consider the sensitivity of any footage used in any training/development scenario.

If you have considered the above and these cannot be met, using this footage for training purposes could be high risk in terms of data protection, and you should complete a Data Protection Impact Assessment (DPIA) to consider the risk and determine if its use is justifiable. Information on DPIAs can be found via the below link:

https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/privacy-reform/data-protection-impact-assessments-dpias/

For more information on individual cases, please refer to the Information Security and Services Team (<u>FMB</u>).

Additionally, material which is still subject to any legal proceedings or where it has been used in a recent prosecution must not be used for training purposes.

Showing footage for training which is highly emotive, challenging or distressing has the potential to cause harm to both prisoners, staff and in some circumstances prisoner's family members. Governors must consider the sensitivity of any footage used in any training/development scenario.

Staff captured in the footage must give their express permission for its use in training and this must be recorded in the risk assessment for retention of material. Staff may agree but conditional to the images being redacted but where staff decline this permission then the footage must not be used. Similarly, if staff withdraw their consent for the use of footage containing their images the footage must be withdrawn from training.

Where training footage contains prisoners' images and the intended use is within the prison for staff training purposes for HMPPS employees only in that event, the prisoner does not need to give permission.

Where the intended use is external to the prison or for prisoner training then the prisoner must either give permission or the images must be pixelated.

### 3.2 Prisoner development

BWVC footage may provide an opportunity for staff to encourage prisoners to reflect on their behaviour, thinking or application of offending behaviour learning.

Staff should carefully consider the potential impact on the prisoner especially where the footage is of a distressing nature. Based on the currently available evidence, it is strongly recommended that use of BWVC footage of people under the influence of Psychoactive Substances is not used as a means of trying to bring about changes in drug-taking behaviour. Examples where footage may have potentially positive effect on the future behaviour might include incidents where a prisoner has been volatile or confrontational towards another prisoner or member of staff.

### 3.3 Legal Privilege/confidential communications

Users of BWVC must be careful to respect legal privilege/confidential communications and must not deliberately record material that is or is likely to be subject to legal privilege or to which confidential access has been given (see the list in paragraph 2.22 of PSI 04/2016). Where images are inadvertently captured, and the footage is to be retained (for example incidents involving use of force) then these images must be edited, redacted, or pixelated.

### 4. Data Management

### 4.1 Copying/saving footage to storage media (DVD disc or USB Flash Drive)

If there is a requirement to copy BWVC material then this will be completed by one of the BWVC administrators, copying the material to a storage media on the stand-alone desktop computer using the BWVC software.

All burning of material to storage media will be recorded and justified and then the storage media(s) securely stored and controlled in accordance with the DPA (2018). Further guidance can be found in PI 2018-02 - Records, Information Management and Retention Policy.

No BWVC material will be copied or loaded to any other storage media other than as described above, without the express authorisation of the Governor.

### 4.2 Disclosing footage for criminal evidential purposes

Where material is being disclosed to the Police pursuant to a criminal investigation; evidence should be shared digitally, via the secure sharing feature within digital data management platform; where possible; where this is not possible, a secure courier service should be used. Two copies of the material must be burned to a disc or USB flash drive, one labelled "Master Copy" and sealed in a signed evidence bag and one "Working Copy" also sealed in a separate signed evidence bag— the two copies must be recorded in the establishment evidence log, detailing:

- The seal numbers
- The BWVC user details
- The time date of recording
- The full name of the person making the duplicate copies
- The full name of the person sealing in the evidence bags

Having stored the evidence in a secure store the evidence log must maintain an accurate log of the time, date and location of storage.

The material can be handed to the police either as a voluntary disclosure or in cases of difficulty or where advice is needed in complex cases, the Operational Partnership Team (OPT) at HMPPS Headquarters can be contacted for advice and guidance. Further guidance can be found in the Dealing with Evidence PSI 2016-08 and the Crime in Prison Protocol

When the copies are handed to the police, they must be signed out of the evidence store and the log duly notated with names/shoulder numbers of the person taking the evidence.

The onward storage location of the discs must also be recorded in the establishment evidence log for Information Commissioner's Office audit purposes.

It is imperative that the prison can demonstrate the integrity of the evidence and that the evidence chain of custody is maintained.

The original footage must be tagged and stored until conclusion of any court process and appeal; the risk assessment for retention will evidence the need for criminal investigation.

### 4.3 Disclosing footage for Intelligence purposes

Where material is being disclosed to the Police for intelligence purposes; evidence should be shared digitally, via the secure sharing feature within digital data management platform; where possible. Where this is not possible one copy of the material must be burnt to a disc or USB flash drive and sealed in a signed evidence bag and recorded in the establishment evidence log detailing:

- The seal numbers
- The BWVC user details
- The time date of recording
- The full name of the person making the duplicate footage.
- The full name of the person sealing in the evidence bags

The material can be handed to the police as a voluntary disclosure or via an Operating Partnership Team 1 application and a note made in the evidence log.

The Governor may decide to consider handling restrictions requiring the police to seek approval should they consider using the footage for any purposes other than intelligence purposes.

The National Intelligence Analysis Unit (Directorate of Security, Order and Counter Terrorism) may require material obtained from the BWVC to support the development of intelligence assessments or in response to intelligence requirements / tasking.

All requests must be authorised by the relevant Head of Regional/Tactical/Strategic/Agency Intelligence (Band 9 or above) and the following details should be provided:

- How the material will be used
- How it will be disclosed (and to whom)
- How it will be stored
- How long it will be stored

The Head of Intelligence (Regional/Tactical/Strategic/Agency) will assume responsibility for ensuring that the material is stored, used and shared appropriately (in full consideration of any handling restrictions imposed by the Governor).

Where material is being disclosed to the National Intelligence Analysis Unit one copy of the material must be burnt to a disc and sealed in a signed evidence bag and recorded in the establishment evidence log detailing:

- The seal numbers
- The BWVC user details
- The time date of recording
- The full name of the person making the duplicate footage
- The full name of the person sealing in the evidence bags

### 4.4 Disclosing footage to the Prisons and Probation Ombudsman (PPO), Her Majesty's' Inspectorate of Prison s (HMIP) or the Independent Monitoring Board (IMB).

Where a matter is subject to an investigation and the PPO, HMIP or IMB has become involved, Governors must ensure there are systems in place to download and retain footage where a serious incident has taken place.

Incidents which should be considered as serious include, but are not limited to:

- Those involving use of force
- Where a crime may have been committed (assault, damage to property etc.)
- Prisoner indiscipline (passive and concerted)
- Hostage or barricade incidents
- Where a complaint or allegation of staff misconduct has been made

Establishments should not assume what footage will be relevant to the PPO, HMIP or IMB investigation, all footage relating to an incident should be retained to allow for PPO, HMIP or IMB investigation consideration.

Where the material is being disclosed to the PPO, HMIP or IMB as part of an investigation into a complaint, evidence should be shared digitally, via the secure sharing feature within digital data management platform; where possible. This process should be completed without causing delay to the PPO, HMIP or IMB investigator, where possible disclosure issues arise the PPO, HMIP or IMB investigator should be consulted on possible redactions or handling restrictions on the footage.

Footage must be checked to ensure it does not compromise the security of the establishment such as disclosure of keys or locks.

Images of staff, prisoners or third parties unrelated to the incident must be redacted.

Where physical copies are being provided, one copy of the material must be burnt to a disc or USB Flash drive and sealed in a signed evidence bag and recorded in the establishment evidence log detailing:

- The seal numbers
- The BWVC user details
- The time date of recording
- The full name of the person making the duplicate footage
- The full name of the person sealing in the evidence bags
- The full details of the person the evidence is being sent to

The establishment must be able to demonstrate robust control of all footage and a clear audit trail to demonstrate integrity of any disclosed material.

The establishment will retain the original footage on the hard drive of the system, tagged and stored; the risk assessment for retention evidencing the need for PPO investigation.

The establishment must retain the original footage on the BWVC system until the conclusion of any investigation and any associated proceedings (such as criminal court or civil disciplinary outcomes) and relevant appeals are finalised.

## 4.5 Disclosing footage to the Prisons and Probation Ombudsman as part of a Death in Custody investigation

Evidence should be shared digitally, via the secure sharing feature within digital data management platform; where possible. Where this is not possible, a secure courier service should be used. Where the physical copies are to be produced relating to a Death in Custody two copies must be burnt to disc or USB flash drive one labelled "Master Copy" and sealed in a signed evidence bag and the other labelled "Working Copy" and sealed in a signed evidence bag two additional copies should be made and labelled "Police" and "Prison and Probation Ombudsman". All copies must be recorded in the establishment evidence log, detailing:

- The seal numbers
- The BWVC user details
- The time date of recording
- The full name of the person making the duplicate footage.
- The full name of the person sealing in the evidence bags
- The discs are securely retained in the document bundle as soon as practicable after the incident

The establishment must be able to demonstrate robust control of all footage and a clear audit trail to demonstrate integrity of any disclosed material.

All original footage located on the system must be tagged and retained until the conclusion of any investigation and any associated proceedings (such as criminal court or civil disciplinary outcomes), including relevant appeals are finalised. Justification for retention will refer to the PPO investigation.

Staff are advised to refer to Chapter 12 of PSI 64/2011 Safer Custody for guidance in collating and managing the document bundle and the disclosure for the PPO.

### 4.6 Disclosing footage to an internal investigator as part of a Disciplinary Investigation

Evidence should be shared digitally where possible; via the secure sharing feature within digital data management platform; where possible. Where this is not possible, a secure courier service should be used. Where material is being disclosed to an internal Investigating officer pursuant to a disciplinary investigation; two copies of the material must be burnt to a disc or USB Flash Drive, one labelled "Master Copy" and sealed in a signed evidence bag and the other labelled "Working Copy" and sealed in a signed evidence bag. Both copies must be recorded in the establishment evidence log, detailing:

- The seal numbers
- The BWVC user details
- The time date of recording
- The full name of the person making the duplicate footage.
- The full name of the person sealing the evidence bags

Having stored the evidence in a secure store the evidence log must maintain an accurate log of:

- The time date and location of storage
- Access to the specific evidence

The original footage on the digital data management system will be tagged and stored until the conclusion of any investigation, associated outcomes (such as disciplinary process) and appeals are concluded; the risk assessment for retention will evidence the need for internal investigation.

### 4.7 Disclosing footage as part of an adjudication hearing

Where material is required for adjudication purposes the evidence should be shared digitally where possible, via the secure sharing feature within digital data management platform. Where this is not possible one copy of the material must be burnt to a disc or USB Flash Drive and sealed in a signed evidence bag and recorded in the establishment evidence log detailing:

- The seal numbers
- The BWVC user details
- The time date of recording
- The full name of the person making the duplicate footage
- The full name of the person sealing in the evidence bags

The material can be handed to the Adjudicator and a note made in the evidence log.

The reporting officer should prepare a summary of the evidence contained in the BWVC footage and identify the persons within it. It is not appropriate for the prisoner to identify themselves in the footage as the evidence may be contested. When viewing evidence of a prisoner's behaviour especially where the prisoner is believed to have taken a substance Adjudicators may consider it too distressing for the prisoner to view and may offer the prisoner the option of declining to view the footage. The Prisoner discipline procedures (PSI 05/2018) provides further detail on evidence for adjudications.

Copies of BWVC footage forming part of the evidence in an adjudication must not sent to any third party. Arrangements must be made for the accused prisoners (and legal advisors or representative where present) to view the evidence at the prison. Failure to allow such evidence to be viewed is likely to lead to any guilty finding being quashed.

However, if the risk of disclosing the information to the prisoner and their lawyer is not acceptable or appropriate for security or operational reasons then it cannot be used as evidence to support an adjudication. Also, the footage may only be disclosed where this is done in accordance with the DPA, particularly where images are captured of not only those subject to the adjudication but anyone who is unrelated to the incident and just happen to be present in the vicinity. This would be applicable to staff, prisoners and any third party and any disclosure could require the consent of the individual concerned or editing/pixelating footage. Consideration can also be given to editing/pixilating footage to remove images of those not involved in the incident, see editing/pixilation section for further guidance.

Once the hearing is concluded to an outcome the disc, USB flash drive or electronic copy of footage must be retained must be retained until it is confirmed that all potential uses of it, including appeal mechanisms have been completed.

Further information on adjudication procedures can be found in PSI 05/2018 Prisoner Discipline Procedures (Adjudications)

### 4.8 Third party requests - Subject Access Requests

Chapter 3, section 45 of the Data Protection Act 2018 gives individuals the right of access to their own personal data, usually referred to as Subject Access Request (SAR). It provides that a data subject is entitled to obtain from the controller —

- a) confirmation as to whether personal data concerning them is being processed, and
- b) where that is the case, access to the personal data and the information on the processing of this data.

They are also entitled to have communicated to them in an intelligible form the information held. Such information requests could include material obtained using BWVC and should be handled in accordance with establishment policies, procedures, and codes of practice.

Users should be aware of the rights of individuals to request BWVC material and Governors should provide guidance for staff and prisoners to enable a request via the SAR process and the time limits therein. Details can be found in the Information Requests Policy Framework.

### 4.9 Footage Redaction / Pixilation

BWVC devices are primarily designed to record incidents involving staff, prisoners, and members of the public. In addition to recording video and audio, they also employ wide angle lenses that capture events across a broad field of view. This can result in the capture of much larger amounts of information than the User intended.

A short recording from a BWVC device can provide compelling evidence for any subsequent debrief or investigation. However, such recordings are also likely to contain information that while not crucial to an investigation could still be considered sensitive in nature. If any of the recorded information is accessed by an unauthorised third party then this could not only compromise an investigation, but also risks causing considerable intrusion into a person's privacy at a time of vulnerability and risk reputational damage to the organisation.

Small traces of sensitive information may have little significance when considered independently. However, when linked together over an entire recording timeline the significance of multiple small pieces of information can be considerable.

At times, it will be necessary to provide copies of BWVC recordings to third parties either for

Investigative purposes such as evidence for partner agencies within the criminal justice system or through a Subject Access Request (SAR). As BWVC devices can capture large amounts of visual and audio data consideration must be given to requirement for redaction/pixilation prior to distribution.

In the case of a SAR a Data Subject is entitled to their personal data, they are not entitled to another person's personal data especially if this could cause that person harm. In cases involving disclosure to PPO, HMIP or IMB images and audio captured of those not directly involved in the incident should be removed prior to disclosure.

It is not possible to restrict or control how the Data Subject shares the information provided to them. It is important to presume that the information released from our control could be posted on social media and quickly reach a potentially global audience.

Redaction covers the editing, censoring, or obscuring of those parts of a recording that could unwittingly reveal sensitive information, expose tactics, or compromise operational strategies. On a practical level this could mean trimming the length of the original recording, concealing, or masking specific visible objects and actions as well as muting parts of the audio track.

When releasing material, care must be taken to review the footage and ensure that only the subject of the incidents image is revealed, and consideration given to removing the identity of staff, other prisoners, and person(s).

Care must also be taken to ensure that no footage presenting a risk to the security of the establishment is released. This could include, but not limited to, disclosure of keys, locks or anything else that may compromise security or the good order and discipline of the establishment.

Any requests for footage taken by BWVC from offenders, visitors or staff should be sent to the Data Access and Compliance Unit (DACU) for processing in line with the existing procedures set out in Information Requests Policy Framework.

When dealing with requests disclosure footage where redaction or pixilation is required advice can be sought from the Pixilation Team (PixilationTeam@justice.gov.ukmailto:PixilationTeam@Justice.gov.uk) to assist with the completion of the task or provide additional guidance on what the establishment should consider when redacting or pixilating footage.

### **5 Operational Scenarios**

### 5. 1 Use of Body Worn Video Cameras Outside of an Establishment

Where an establishment intends to deploy staff equipped with BWVC outside of the establishment itself (such as during external prisoner escort, hospital escort, bedwatch or establishment perimeter patrols) the use and rationale must be documented within the establishment LSS.

A BWVC can capture a large amount of sensitive information that may have no evidential value but if lost or disclosed could have a negative impact on members of the public as well as reputational damage to the organisation. The activation of cameras outside of the establishment should be used minimally and proportionately to circumstances or incident intended to be captured.

As provided in section 3.2 of this guidance, at the point of starting to record BWVC users must ensure that they make an audible announcement that BWVC is in use and manage any objections to being filmed as soon as it is possible to do so.

When using BWVC outside of an establishment the BWVC user should be conscious they are potentially capturing data (audio and video) of members of the public who may be unaware they are being recorded. To minimise the potential for this type of collateral intrusion and limit the potential requirement for footage to have to be pixilated or redacted the BWVC user should consider ceasing recording at the earliest opportunity once an incident is resolved.

As provided in section 3.8 of this guidance, any objection to being filmed must be addressed by the BWVC user with a clear and concise explanation why recording is taking place. The user may also explain that non-evidential material is only retained for a maximum period of 90 days and that any access to the material is both limited and controlled and in the case of a complaint to write to the Governor.

### 5.2 Spontaneous Use of Force (UoF)

The use of a BWVC is a proportionate means of corroborating the facts during any type of incident or situation where the use of force appears to be likely, or where force is being applied. The footage of the incident can prove invaluable during later review and can demonstrate transparency in respect of actions undertaken or not undertaken. Users should consider their training in Spontaneous Protection Enabling Accelerated Response (SPEAR) and other personal safety training to recognise at the earliest opportunity that a situation is escalating and activate their BWVC. The activation of BWVC may itself act to de-escalate an incident.

In the rare situations where it is difficult to commence recording prior to force being applied, such as when users face spontaneous and /or unexpected violence for example, the user should activate the BWVC as soon as it is practicable to do so, thus enabling the 'pre-record' facility on the BWVC to capture the maximum amount of incident footage. In such circumstances users should explain why earlier recording was impracticable on the BWVC device and within their written statement.

Users must be aware that:

- The BWVC is unlikely to capture the whole circumstances of the incident
- The BWVC recordings are unlikely to justify in isolation the reasonableness necessity or proportionality of force used

Users must justify their actions, perceptions, and decisions as per normal within their written Use of Force statement. The writing of UoF statements must be completed before any captured footage is viewed, this will enable staff to detail the threat perceived at the time of the incident and not on reflection having viewed any footage. Staff must reference BWVC footage was captured within the UoF statement. The use of BWVC is a tool to support and not replace written statements. If footage is viewed following the writing of the UoF statement and the user wishes to make a further statement, this can be provided as an addendum to the original statement, clearly stating this is being provided following viewing the footage.

BWVC footage of UoF must be tagged and retained in line with UoF paperwork.

### 5.3 Planned Use of Force (UoF)

The member of staff planning this type of physical intervention must prioritise the use of their handheld video cameras where available and not rely solely on BWVCs.

Where the circumstances require a swift intervention to safeguard the wellbeing of a person(s) then the senior staff member at the scene can make the decision to use only a BWVC to record the intervention. There must be a clear rationale given in the UoF/IRS documentation to account for the decision to use BWVC over hand-held video camera equipment.

The use of BWVC in addition to hand-held video cameras, may provide additional helpful material. The on-scene member of staff planning the intervention will consider the circumstances and decide whether BWVC is to be deployed or not and will communicate their decision to BWVC users prior to the start of the Operation and will make a justification statement on the recording. This will ensure transparency and will be available to others to understand later the rationale for the decision. BWVC footage capturing UoF must be tagged and retained in line with UoF paperwork.

National Technical Response Group (NTRG) and National Dog Technical Support Group (NDTSG) have separately issued BWVC's with separate facilities for downloading footage outside of an establishment.

### 5.4 Nights

The standard operating procedures for Nights will also present the need for incident management and conflict resolution. The wearing of BWVC by all Night staff (including Band 2 OSG staff) will provide support in the early stages of incident management particularly in the moments before the arrival of the Night manager and supporting staff. Audio and visual footage will assist in the laying of adjudication charges, police referrals internal investigations and ongoing incident management.

### 5.5 Incident Response – areas where visitors/members of the public are present

BWVC are authorised to be used in all prisons which includes the use in Domestic/Legal visits area, or the Visitors Centre so long as legal visits are not recorded.

BWVC users must ensure that they make an audible announcement that BWVC is in use and manage any objections to being filmed as soon as it is possible to do so.

In the event of a member of the public wishing to make a complaint, the BWVC user should advise the person that they can do so in writing and to the Governor.

Managers may consider it prudent to retain any footage involving members of the public or visitors for the 90-day or set period thereafter with reasons set out in the justification assessment.

### 5.6 Incident Response – Medical Intervention

The use of BWVC to record footage is mandated to be "incident related" – which is therefore likely to include incidents involving injury to or illness of a prisoner. This may also include situations where medical interventions are taking place.

On attending an incident involving medical intervention BWVC users must consider any sensitivities of the circumstances. This is particularly relevant when attending an incident where a prisoner is receiving lifesaving medical intervention and therefore is unable to be informed of, or consent to, being filmed. Users should conduct a dynamic risk assessment and where no threat to the safety or security of others exists users, should maintain audio capture to record any decisions and rationales during interventions, but should consider non-intrusive capturing of the medical intervention. This may be through directing the camera lens away from intervention.

The BWVC user will record the necessity, proportionality, and justification for their actions in the accompanying written documents.

#### 5.7 Routine Medical Treatments

Where an incident occurs during routine medical treatment it may be appropriate for BWVC users to commence recording. For example, a Segregation Unit officer wearing a BWVC who is

accompanying a Nurse on Segregation rounds would not routinely record the interaction with a prisoner. However, this would not be the case if the prisoner became hostile and confrontational. Similarly, where a Nurse is dispensing medicines at the treatment hatch it would not be appropriate for recording to routinely take place, but should the prisoner become volatile then it would become appropriate to start filming. Recording of footage in these circumstances would primarily be to influence and improve the behaviour of the prisoner but could also be used for internal disciplinary purpose if required.

### 5.8 Dogs Teams & Dedicated Search Teams

Specialist teams have local arrangements for the distribution and storage of issued BWVC units. Due to the dynamic nature of their work and increased potential risk of spontaneous Use of Force incidents, specialist teams entering establishments may use BWVC during the initial phase of their searches to show the behaviour of the prisoner, approach of the staff in completing the search and show the initial condition of the cell.

On the completion of the search BWVC cameras should be docked to allow footage to be downloaded to the centralised storage system. This footage should be retained in line with the data retention principals outlined in this guidance in case of subsequent complaint regarding the staff approach or the condition of the cell.

Additionally, where these teams are conducting perimeter searches relating to `Throw Overs` (such as members of the public throwing contraband over the fences / walls into establishments) may use BWVC's to assist with evidence gathering to assist with potential prosecutions or detaining individuals outside of the establishments.

### 6. System Management

The governing Governor is responsible for deciding who within the establishment will fulfil the following roles and ensuring they are sufficiently competent to fulfil the role.

Identified roles and responsibilities

- 6.1. User the person wearing the BWVC unit is responsible for:
- Self-assigning a BWVC with an RFID swipe-card or sticker
- Checking that the BWVC has no visible damage and that the equipment is working correctly and is set to "pre-record" mode ready for use
- The safe keeping of the BWVC while in their possession ensuring it is not left unattended and is to remain in their possession until the user has returned it to the docking system and booked back in
- Recording footage whilst wearing it
- Returning the BWVC firmly to a slot at the end of their shift
- Entering a note in the log that footage of an incident or event has been captured providing as a minimum date/time/prisoner name, number/staff name/subject or not to an adjudication
- Promptly reporting any damage or non-functioning equipment
- 6.2. User/View footage the person wearing and requiring access to view footage; this person is likely to wear the BWVC and have the need to view footage to make incident management decisions. The access will be limited to "view" footage only.

- 6.3. Administrator the person(s) with ability to tag, digitally disclose and burn footage to disc or USB flash drive is responsible for:
- Checking the BWVC user log
- Collating and recording the information for the justification risk assessment
- Ensuring that incident/event footage once approved is tagged
- Where required the burning of footage to disc
- Pixilation of footage as required
- Robust management of chain of evidence log
- 6.4. Approval Officer– the person authorising the justification assessment responsible for:
- Authorising the data to be retained past the 30 day auto delete point
- Setting the period to review the retention justification
- Ongoing justification of data retention
- 6.5 System Owner the person with the ability to tag, burn, add new users and delete footage:
- Is likely to be a Senior Manager/Functional Head and will have the overall responsibility for the system and the Data recorded and retained
- Person identified in signage as the establishment point of contact
- Assigns the responsibility to administrate the system and oversee the safe keeping of the BWVC equipment

### 6.6 Assigning Users

Governors must carefully consider the deployment of the equipment and staff designated as users. Deployment should be on an informed basis determined in conjunction with the Violence Reduction Tool available on the Performance Hub on the Intranet.

Staff must complete the required training and understand the principles on use of BWVC equipment within 90 days of first drawing a camera.

### 6.7 Equipment Management

Governors must carefully consider how to appoint the system management/oversight roles to ensure robust management of the system, equipment and consistent and compliant approach to the retention of footage and data management.

Governors must ensure that the BWVC equipment is stored securely and that robust checking measures are implemented to ensure that each unit is strictly accounted for. These checks must include an auditable regular checking procedure to enable:

- Missing units to be identified at the earliest opportunity
- Faulty units to be identified and reported

Any loss of BWVC equipment must be reported on IRS.

The incident must be entered as soon as possible, incidents must be entered on IRS within 24 hours for a telephone reportable incident and within 72 hours for all other incidents.

The loss of BWVC equipment will also require reporting as a "Data Loss". The Information Security Policy Framework Annex B provides guidance for this.

Governors must implement a local process to give assurance that the log correlates with actual use.

The software supplied undertakes automatic routine "health" checks confirming battery charging levels, meta data check (date and time) and a system diagnostic check to ensure the footage is routinely downloaded.

The software supplied with the equipment contains an automatic asset management function with capacity to maintain a central record of all BWVC devices issued to members of staff.

### 6.8 System access

Each establishment must ensure that all access to the data management system and recorded footage is managed, logged and robustly controlled.

Access levels must be carefully attributed and limited to maintain the integrity of the system.

Data edit functionality must be restricted to a senior member of staff, the designated "Owner" of both System and recorded data.

Footage must be viewed in isolation of staff areas with obscured sight lines and where audio access is facilitated via headphones.

### 6.9 Documentation

Establishment User log must capture the following information

- Date and approximate time of capture
- User identity
- Location of incident/event
- Persons involved
- Brief description of incident/event
- Adjudication charge laid

### 6.10 Justification assessment must set out the following information

- Date + reference number for justification assessment
- · Brief outline of captured footage
- Reason for retention required for UoF/Adjudication/DiC/Complaint/Investigation etc
- Requirements for disclosure, include details of who disclosed to.
- Footage copied to disc or USB flash drive

- Date disc to evidence log plus evidence bag reference number
- 6.11 Justification/decision log must capture the following information
  - Date and reference number for justification assessment
  - Retention decision
- 6.12 Evidence log must capture the following information
  - Date and time
  - Evidence bag number
  - Brief description of evidence
  - Audit trail of access/removal from safe