National Offender Management Service

National Security Framework SECURITY MANAGEMENT Body Worn Video Cameras		**NSF:**
This instruction applies to :-		**Reference :-**
Prisons – Prison Service Instruction (PSI)		**PSI 04/2017**
Issue Date	**Effective Date**	**Expiry Date**
20 March 2017	20 March 2017	N/A

Issued on the authority of	NOMS Agency Board
For action by	All staff responsible for the development and publication of policy and instructions *(Double click in box, as appropriate)* ☐ NOMS HQ ☒ Public Sector Prisons ☐ Contracted Prisons* ☐ National Probation Service (NPS) ☐ Community Rehabilitation Companies (CRCs) ☒ NOMS Immigration Removal Centres (IRCs) ☐ Other Providers of Probation and Community Services ☒ Governors ☐ Heads of Groups ☐ NOMS Rehabilitation Contract Services Team **** If this box is marked, then in this document the term Governor also applies to Directors of Contracted Prisons***
Instruction type	*Delete as appropriate* - ***delivery of non-specified service/service improvement/ /legal compliance***
Provide a summary of the policy aim and the reason for its development/revision	The aim of this policy is to provide instruction and guidance to prisons in the use of Body Worn Video Cameras and the management of the data captured.
Contact	Ceri Mortimer ceri.elaine.mortimer@hmps.gsi.gov.uk 020 193 5881
Associated documents	Related Service Specification Related Operating Models Related Direct Service Costs and Assumptions paper Related Cost Spreadsheets NOMS directory of service specifications can be found at https://www.gov.uk/government/collections/noms-directory-of-services-specifications PSI 47/2011 Prisoner Disc`ipline Procedures PSI 09/2014 Incident Management PSI 64/2011 Management of Prisoners At Risk of Harm to

	Self, to Others and From Others PSI 11/2012 Incident Reporting System PSI 24/2014 Information Assurance Policy PSI 22/2012 Covert Surveillance PSI 35/2014 Records, Archiving, Retention and Disposal PSI 44/2014 Data Protection Act 1998 & Freedom of Information Act 2000 Environmental Information Regulations 2004 PSI 02/2012 Prisoner Complaints PSI 15/2011 Management of Security at Visits PSI 16/2011 Providing Visits & Services to Visitors PSO 1300 Investigations PSI 01/2016 Corruption Prevention – How to Identify, Manage and Report Staff Corruption in Prisons and Headquarters PSI 04/2016 The interception of Communications in Prisons and Security Measures
Replaces the following documents which are hereby cancelled: None	
Audit/monitoring: Mandatory elements of instructions must be subject to management checks and may be subject to self or peer audit by operational line manager/contract managers/HQ managers as judged to be appropriate by the managers with responsibility for delivery. In addition NOMS will have a corporate audit programme that will audit against mandatory requirements to an extent and at a frequency determined from time to time through appropriate governance.	
Notes: ***All Mandatory Actions throughout this instruction are in italics and must be strictly adhered to.***	

CONTENTS

1. Executive summary

1.1. This PSI sets out the policy and legislative framework with respect to the planning, introduction and use of Body Worn Video Camera equipment and the management and retention of audio and visual data produced by BWVC.

1.2. This instruction is one of a number of Prison Service Instructions (PSIs) which form part of the Security Management function of the National Security Framework (NSF). All Security Management instructions can be accessed via the National Security Framework within the NOMS intranet. This PSI supports the Security Management specification.

Background

1.3. The use of Body Worn Video Camera (BWVC) technology has been in place for a number of years within a variety of public sector organisations. When used effectively a BWVC allows first person audio and visual images to be captured to provide a clear and irrefutable record of events. With proper use the introduction of this technology will assist with:

- Allowing for more detailed examination of the events leading up to and management of incidents
- Enhance evidence capture
- Promoting positive behaviour and interaction between staff and prisoners
- Developing effective rehabilitative staff/prisoner relationships; supporting transparency, trust and confidence between staff and prisoners

Desired Outcomes

1.4. BWVC will only be used for overt recording and in order to support:-

- De-escalation of conflict or confrontation
- The prevention or detection of crime and disorder
- The apprehension and prosecution of any person who has committed a crime within a prison (including the use of images as evidence in criminal proceedings)
- Safe resolution of internal staff disciplinary investigations
- Improving public and employee Health & Safety
- The protection of staff, visitors and prisoners
- Safeguarding the security of the establishment
- Development of staff skills through use of operational footage for training purposes

Application

1.5. The NSF incorporates mandatory requirements derived from specifications relevant to its specific policy areas.

1.6. Staff designated by the Governor/Director within a prison/Young Offender Institution (YOI) will be required to wear a BWVC. This PSI applies to all Public Sector Prison establishments and to all staff working in a prison.

1.7. This PSI is seen as guidance for Contracted out establishments where Body Worn Video Camera technology is deployed or where they are contemplated by the private provider

Mandatory Action

All mandatory elements of this instruction are specified by the use of italic typeface.

1.8. *Governors must ensure that they review their Local Security Strategies to ensure they are in accordance with the instructions set out in this PSI and agreed with the Deputy Director of Custody or Executive Governor or equivalent.*

1.9. *Governors must ensure that contingency plans and incident management are reviewed to include the necessity to secure all digital footage promptly.*

1.10. *Governors must ensure robust management of the BWVC equipment, system and data management.*

1.11. *Governors must ensure that the stand alone computer system is situated in a secure location with limited staff access to allow for footage to be viewed by appropriately approved staff out of sight and sound of others.*

1.12. *Establishments must have an identified manager and an identified deputy to take on the role of "Approver" for retention of footage past the 3 month[1] point, whose role will also include managing the process and system in accordance with all necessary legal and policy requirements.*

1.13. *In those establishments where it is authorised for use and available, BWVC must be deployed and set to record during a response to any reportable Incident.*

1.14. *In those establishments where it is authorised for use, BWVC must be issued to appropriately trained staff for use both during "patrol state" and "night state" of the establishment.*

1.15. *Establishments must have local contingency plans outlining the necessity to secure all digital footage. This can be achieved by prompt uploading of the footage to the secure server. Retention of the footage will be managed in line with this instruction.*

1.16. *The use of a BWVC must be wholly overt*.

1.17. *Establishments must ensure that prisoner and staff induction programmes state the intention to film where circumstances require it. Induction programmes must contain information setting out the reasons for use of BWVC and the potential uses of captured footage.*

1.18. *Establishments must ensure adequate signage is in place in all areas to include Domestic and Legal Visits and Visitors' Centres stating that BWVC equipment is in use and that both audio and visual recordings are made.* These signs should also highlight the establishment point of contact in case of queries and complaints.

1.19. *The use of BWVC in legal visits areas must be operated within the mandatory policy that such visits are conducted within sight but out of hearing of staff. The Body Worn Video Camera must not be used to record legally privileged conversations.*

1.20. *The procedures outlined in this document must be considered as a minimum standard for the use of BWVC equipment and should be used as a basis for the construction of establishment-specific policies and operating procedures*.

[1] To comply with Prison Rule 35D Retention of material; see definitions para 2.3

1.21. *No Member of staff must be assigned to wear or use BWVC without having undertaken the required training.*

1.22. *All staff must make themselves aware of the content of this PSI.*

Resource Impact

1.23. There may be some resource implications for some establishments in the use of BWVC to ensure that they are used in accordance with legislation and the requirements set out in this PSI. Due to the variations in the types of prisons and numbers of units allocated and purchased resourcing is difficult to quantify. Governors may contact Public Sector Prisons Business Development Group and Contracted providers may raise issues through contract management meetings.

(Approved for Publication)

Claudia Sturt
Director of Security, Order and Counter Terrorism, NOMS

2. Operational Instructions

The use of Body Worn Video Cameras (BWVC) is for internal use within the confines of a prison establishment (see para 2.3 below).

Legislative Framework

2.1. Specific detailed instructions for the use of audio/visual recording technology storage and use of footage is contained in the PSIs listed below:

- PSI 22/2012 - Intelligence – Regulation of Investigatory Powers Act: Covert Surveillance
- PSI 35/2014 – Records, Archiving, Retention and Disposal
- PSI 44/2014 – Data Protection Act 1998, Freedom of Information Act 2000, Environmental Information Regulations 2004
- PSI 64/2011 Safety Custody
- PS0 1300 Investigations

Overview

2.2. Particular consideration has been given to the following legislation in the drafting of policy and in turn should inform the planning, introduction and use of BWVC:

- Data Protection Act (DPA) 1998: details the regulation of the processing of information relating to identifiable living individuals, including how this information is obtained, held, used and disclosed
- Freedom of Information Act 2000 (FOIA): provides for the disclosure of information held by public authorities or by persons providing services for them
- Human Rights Act 1998: provides rights and freedoms guaranteed under the European Convention on Human Rights (ECHR)
- Regulation of Investigatory Powers Act (RIPA) 2000: details, in part, directed and intrusive surveillance
- Criminal Procedures and Investigations Act 1996: covering the disclosure of material in criminal cases
- Protection of Freedoms Act 2012: details, in part, the destruction, retention, use and regulation of evidential material, provides for a code of practice for surveillance camera systems and the appointment of a Surveillance Camera Commissioner
- Surveillance Camera Code of Practice: is issued by the Secretary of State under Section 30 of the Protection of Freedoms Act 2012 Act and provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities
- Surveillance Camera Commissioner: Self Assessment tool: testing the compliance with the 12 guiding principles of the surveillance camera code of practice

Definitions

2.3. For the purpose of this document the following definitions apply:

- Prison establishment - defined as “within the secure perimeter of the Prison including the gate lodge”. Where operationally necessary the BWVC can be worn in any staff response to an incident external to the prison from within the prison including prison car park or Visitors Centre or to any area part of an established routine perimeter check.
- BWVC – Body Worn Video Camera: a body-worn device worn overtly by trained and authorised staff for the primary purpose of capturing digital footage both visual and audio

- Overt - if the user is open about their intentions to record audio and visual footage
- Covert - if, and only if, recording is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is, or may be, taking place
- User – a member of staff trained and authorised to use BWVC equipment in a Prison establishment
- Tagged footage – where justification has been made to retain digital footage past the automatic 3 month deletion point
- 3 month initial storage period – this period complies with 35D of the Prison Rules 1999 (retention of material) - for the purposes of setting the digital system this will be set to a 92 day point from date of footage capture

Overarching principles

2.4. The use of a BWVC will allow a more detailed examination of the events leading up to and the management of incidents and particularly those which may have resulted in the use of force. It is a useful means to record material and to demonstrate transparency in respect of the actions undertaken or not undertaken by the user, other members of staff and prisoners.

2.5. It is expected that where BWVC is present at any reportable incident (ref PSI 11/2012 Management and Security of the Incident Reporting System) it will be used to capture both audio and visual footage until the safe and secure conclusion of the incident.

2.6. Any use will be recorded as a minimum in the log and also in any subsequent documentation such as Use of Force, Adjudication, Incident Report System, Intelligence report F213 injury to prisoner.

2.7. *Where BWVC is deployed within a prison it must be used:*

- *When a user has or may be required to exercise force against a person or persons (refer to para 2.8)*
- *When a user believes an interaction presents or is likely to present a risk to the safety of the user, other members of staff prisoner or other persons present*
- *When a user is responding to an alarm bell or Incident*
- *When a user considers the use of BWVC to be a necessary and proportionate means of recording any other interaction or event*

2.8. *If the user of BWVC equipment is involved in any form of incident or event where filming would normally occur but such filming does not actually take place, for example because the incident happened too quickly and concluded before activation of BWVC was possible they must detail the reasons for not recording the incident in their accompanying written statement.*

2.9. *BWVC must not be used:*

- *Covertly*
- *To record general working practices*
- *To record interactions without specific cause*
- *To record the first accounts of victims and /or witnesses at incidents in order to avoid inadvertently conducting an investigatory interview*
- *To routinely record the conduct of any type of search of the person*
- *Outside of the confines of the establishment as defined in para 2.3 above*

Professional Standards

2.10. Users should not intentionally obscure the camera lens or fail to record all or part of an incident without exceptional cause/justification. Governors may wish to consider whether such calculated actions including the misuse of the equipment/software, may render the user liable to internal investigation/disciplinary action.

2.11. Any senior member of staff, with express permission from the Governor may access the footage for professional standards or related purposes where there is a clear and justifiable need to do so, including for:

- Quality assurance purposes
- Conducting supervision or assisting with training and professional development
- Identifying establishment-wide or individual training needs
- Investigating specific allegations, specific patterns of complaints and conducting disciplinary investigations
- Where specific intelligence has been received that would indicate that viewing of BWVC footage is proportionate and necessary

2.12. *When reviewing material in any of these circumstances managers and/or investigators must make a note of the fact they have done so and record their reasons for reviewing the material on the retention justification documentation.*

2.13. *Managers must ensure that users do not become overly reliant on BWVC at the expense of existing mechanisms. For example, BWVC must not be used to record a cell search in place of the required second officer. BWVC footage does not replace the need to produce an Incident Report or Use of Force documentation. BWVC is a tool to support and not replace and all other protocols must still be complied with.*

2.14. BWVC is for overt use only but nonetheless there may be occasions when unintentional footage is captured, for example during an incident. *If during any review of material there is any indication of further wrongdoing by **any party** including potential staff misconduct then the matter must be dealt with in accordance with current procedures for such wrongdoing and the footage may be accessed to inform any disciplinary investigation or be disclosed to the Police for criminal investigation.*

2.15. Any incidental footage captured indicating staff misconduct obtained without the express knowledge of the subject cannot be reasonably ignored or disregarded by NOMS and in any event this will be processed in line with the DPA and other obligations.

2.16. Any corruption issues must be reported on Mercury and reported in line with PSI 01/2016 Corruption Prevention- How to identify, report and mange staff corruption in prisons and Headquarters.

3. Operational practice and procedures

Point to start recording

3.1. The initial response to an incident will prompt users to commence recording at the earliest opportunity in order 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"

3.2. 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 en-route capturing footage of the scene and events immediately on arrival.

3.3. *All users must be reminded that the use of BWVC does not replace the need for written statements, Incident Reports or Use of Force statements and any other form of written report. BWVC footage is to support and not replace written statements. All users will be reminded that they must record the justification for the use of the camera in the daily log and any supporting documentation be that Adjudication, Use of Force, Incident Report System or Intelligence Report.*

During Recording

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

3.5. *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 now say and do will be recorded.

3.6. 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 course of 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.

3.7. *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 sufficient coverage of the incident/event or restricting the user's movements and ability to manage the incident.*

3.8. *The use of BWVC in areas where there is a higher than usual expectation of privacy (e.g. toilets, showers, changing rooms, search areas and medical treatment rooms), will require compelling reasons for doing so, for example in response to an incident where the safety or security of others is at risk.*

3.9. Users will be further aware of the sensitivity of using BWVC in places of worship where this may be viewed as disrespectful.

3.10. *Any footage or recording must generally be uninterrupted from the beginning of the incident until the end.*

3.11. Where incidents or events are protracted and there are lengthy periods of inactivity or because of the need to isolate confidential details such as victim details or witness details from the footage, there may be cause to conduct selective filming. *Users should be aware that this could lead to challenge and must ensure that explanation and justification is given for selective recording in the accompanying documents.*

3.12. *Prior to any temporary suspension of recording the user must make a verbal announcement explaining the reason(s) for the suspension and conversely when re-commencing the footage must make a verbal announcement.*

3.13. There may be occasions when recording is inadvertently stopped or disrupted during the course of 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.*

3.14. *Once recording has been competed the data must be retained and handled in accordance with this PSI and the Data Protection Act and established procedures of the establishment as set out in the Local Security Strategy (LSS).*

Cessation of Recording

3.15. *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*.

3.16. *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*

Post recording

3.17. Users will at the end of their duty return the BWVC to the docking station.

3.18. *For each use of the camera users must make an entry in the log providing as a minimum their user details, time, date and prisoners details and whether or not an adjudication charge is being laid.* This log entry will provide the justification for use and record that the camera was used.

3.19. *Post incident/event users will complete supporting documentation in the form of Use of Force, Incident report, Intelligence report or adjudication paperwork in the usual way and indicate whether BWVC was activated*.

3.20. *Where the camera was successfully used to de-escalate a situation then users must make an entry in both the log and on Cnomis case notes to that effect.*

3.21. *Post incident/event Duty Managers must ensure that the presence of BWVC footage is noted in the **I**ncident **R**eport **S**ystem report, on the reporting system, in a prisoners case notes on Cnomis and any resulting **I**ntelligence **R**eport - BWVC will be used to corroborate and not replace evidence from other sources.*

3.22. *Where more than one BWVC is present at the scene of an incident or the area is also covered by CCTV the system administrator and designated Approval Officer must ensure that all available material of the incident is secured as evidence in anticipation of any defence argument that may be presented.*

3.23. All BWVC material should be uploaded on to the secure server as soon as practicably possible; this is completed automatically when the camera is placed in the docking station and will ensure that the audio and visual data is secure.

Partial recording

3.24. 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.

3.25. 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.

3.26. 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.

Transcripts

3.27. 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

3.28. 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 provided, the accompanying footage will be retained.

Dealing with objections to being filmed

3.29. *Any objection by a prisoner(s) or visitor(s) 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.

3.30. The user may also explain that non-evidential material is only retained for a maximum period of 3 months 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 1998 (DPA). Further guidance can be found in PSI 44-2014 DPA 1998, FOI 2000, EIR 2004

3.31. *If the prisoner or visitor continues to object then the user must make a decision 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 also within the accompanying written document.

3.32. An example of such an occurrence may be where filming would record a prisoners intimate body parts. However, there may be occasions where a prisoner is either in a sensitive area such as the showers or is partially clothed but his/her 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.*

3.33. *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.

3.34. 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.

3.35. 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.*

3.36. Equally users may be approached by a prisoner with a request to film a particular 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 a Mercury Intelligence Report.*

<u>Allegations, complaints and Investigations</u>

3.37. 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.

3.38. *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*.

3.39. *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.*

3.40. 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 3 months after recording. If the incident has been tagged for retention then it may be viewed beyond this 3 month period.

3.41. 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.*

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

Post Incident procedures

3.43. 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.*

Scenes of Crime/Preservation of evidence

3.44. *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.*

3.45. In responding to incidents users may arrive in to 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.

3.46. 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.

3.47. 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. Under the current Code of Practice (issued under the Police and Criminal Evidence Act 1984), this does not allow for BWVC to be used to record suspect interviews either voluntarily at/away from a police station or when under arrest.

3.48. Staff should limit the initial questioning in order to:

- Identify if an offence has been committed
- Identify and mitigate against any ongoing or further risks – manage the incident and those involved

3.49. *Establishments must set out in their local contingency plans the necessity to secure all digital footage. This can be achieved by prompt uploading of the footage to the secure server. Retention of the footage will be managed in line with this instruction.*

Staff Training and development

3.50. There will be occasions when staff identify examples of best practice, effective de-escalation skills or incident management. It is entirely a matter for the individual establishment to determine whether such material should be used for training and development. Managers may consider that it would be productive to use such footage for individual/general staff training and development purposes. The footage will need to be

managed in line with DPA principles, risk assessed and justification clearly set out for retaining the footage for these specific purposes.

3.51. *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.*

3.52. 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.*

3.53. *Staff captured in the footage must give their express permission for its use in trainingnd 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.*

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

3.55. 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 redacted.*

Prisoner development

3.56. There may be opportunity for prisoners to have access to footage in order for appropriate staff to challenge behaviour, thinking or application of offending behaviour learning.

3.57. Staff should carefully consider the potential impact on the prisoner especially where the footage is of a distressing nature. Examples where footage may have potentially positive effect on the future behaviour might include incidents of behaviour affected by use of illicit substances or where a prisoner has been volatile or confrontational towards another prisoner or member of staff.

Legal Privilege/confidential communications

3.58. PSI 04/2016 Interception of Communications in Prisons and security measures sets out in paragraph 2.22 the list of legal/confidential communications exempt from interception.
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 protection. Where images are inadvertently captured and the footage is to be retained then these images must be redacted/pixelated.

4. Data Management

4.1. *Governors must ensure auditable management of the BWVC equipment, system and data management.*

4.2. *Establishments must have one or more managers and an identified deputy to take on the role of Approval Officer for retention of footage past the 3 month point, whose role will also include management of the process and overall system in accordance with all necessary obligations. These roles and responsibilities must be communicated to staff in the establishment and set out in the establishments LSS.*

4.3. *Data must be managed robustly and all access, use and movement must be documented in the establishment's evidence log. This log will provide an Audit trail for the Information Commissioners Office at point of inspection.*

4.4. *Users who have recorded any BWVC material must not be given IT permissions to the secure server or authority to delete any data.*

Data Retention and Deletion

4.5. *All staff need to be aware that under the Data Protection Act 1998 (DPA) –personal data processed and held for any purpose must not be kept for longer than is necessary for that purpose. The DPA does not contain any interpretation of that principle, but the retention periods and justification requirements set out in this instruction have taken the requirements of the DPA into consideration.*

4.6. *Establishments must maintain clear decision logs for the retention of all BWVC footage.*

4.7. Once uploaded BWVC material will be routinely stored on the system for a period of up to 3 months at which point unless the footage is tagged it will be automatically deleted.

4.8. To retain footage past the 3 month point a designated Approval Officer designated manager will complete a risk assessment setting out the justification for retaining the footage in line with the DPA.

4.9. The justification assessment will include a brief description of the content, details of the person capturing the footage, date time and place and the reason for retention i.e. Adjudication, Use of Force, Police Referral, Prisons and Probation Ombudsman (PPO) investigation, Disciplinary Investigation, litigation.

4.10. Once the retention justification is made the footage can be stored on the storage system for a maximum period of 6 years from date of incident.

4.11. The DPA requires that the necessity to retain is periodically reviewed to ensure that the justification remains.

4.12. These review periods are set in order to provide assurance that the justification, necessity and proportionality of retaining the footage is considered at appropriate intervals.

4.13. Where the footage is to be disclosed to external partners such as Police or PPO – the footage will be promptly burned to two discs and the establishment's chain of evidence log maintained. The establishment will be responsible for the secure transfer of digital data to Police/PPO or other stakeholders. (ref para 4.23 & para 4.33)

4.14. *Any copies of BWVC material that are produced during the course of any investigation and subsequent legal proceedings, if any, must be retained until the conclusion of proceedings*

and any appeal routes. *When there remains no justification to retain then all copies must be securely disposed of and in accordance with chain of custody, evidence procedures and the DPA.*

4.15. Where BWVC material has been recorded and there is no reason to retain the material, as there are no judicial proceedings anticipated or internal investigations, then the footage will be automatically deleted from the system at the 3 month point. *Footage must not be routinely kept solely for intelligence purposes, for staff training or for prisoner development.*

4.16. There may however be exceptional circumstances where retention is required for intelligence or identification purposes and staff or prisoner development.

4.17. *In such cases a member of the senior management team, a Band 8 or above, must complete a justification assessment setting out the necessity, proportionality and justification for keeping the footage.* This risk assessment will set out:

- Why the circumstances are exceptional
- Why retention is necessary and proportionate
- Regular review intervals at least annually from date of retention
- At each review the rationale for continuing retention.

4.18. The designated Approval Officer will authorise the retention of data and also set the review date to consider ongoing justification to retain, as periods no longer than annually from date of first retention.

4.19. *As soon as it is assessed as no longer necessary, proportionate or justified to retain the material then any copies must be destroyed and it must be deleted from the system in accordance with routine deletion processes.*

Copying/saving footage to disc

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

4.21. All burning of material to disc will be recorded and justified and then the disc(s) securely stored and controlled in accordance with the DPA.

4.22. No BWVC material will be copied or loaded to any other storage media other than as described in para 4.20/4.21, without the express authorisation of the Governor.

Disclosing footage for criminal evidential purposes

4.23. *Where material is being disclosed to the Police pursuant to a criminal investigation; both copies of the material must be burned to a disc, 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 discs*
- *The full name of the person sealing in the evidence bags*

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

4.25. The material can be handed to the police either as a voluntary disclosure or under a lawful obligation for example under a court order. The relevant exemption of the DPA should be noted. Further guidance can be found in PSI 44/2014 Data Protection Act & Freedom of Information Act 2000 Environmental Regulations Act 2004.

4.26. *When the discs 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.*

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

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

4.29. *The original footage on the hard drive of the standalone system must be tagged and stored; the risk assessment for retention will evidence the need for criminal investigation.*

Disclosing footage for Intelligence purposes

4.30. *Where material is being disclosed to the Police for intelligence purposes 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 disc*
- *The full name of the person sealing in the evidence bags*

4.31. 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.

4.32. 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.

4.33. 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.

4.34. *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*

4.35. 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).

4.36. *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 disc*
- *The full name of the person sealing in the evidence bags*

Disclosing footage to the Prisons and Probation Ombudsman as part of a complaint

4.37. *Where the material is being disclosed to the PPO as part of an investigation in to a complaint the footage must be checked by the establishment and signed off for disclosure by BWVC "system owner" before it is disclosed to the PPO investigator.* This will also apply if footage is provided by a third party for example the police.

4.38. *Footage must be checked to ensure it does not compromise the security of the establishment such as disclosure of keys or locks and also to ensure it does not infringe personal rights under the DPA; where images are captured of persons but whose presence is incidental or unrelated to the incident.* This will apply to both staff, prisoners and any third parties.

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

4.40. *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 disc*
- *The full name of the person sealing in the evidence bags*
- *The full details of the person the evidence is being sent to*

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

4.42. 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.

4.43. *The establishment must retain the original footage on the hard drive of the system.*

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

4.44. *Where the footage relates to a Death in Custody two copies must be promptly burnt to disc one labelled "Master Copy" and sealed in a signed evidence bag and the other labelled "Working Copy" and also 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 discs*
- *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*

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

4.46. *All original footage located on the hard drive of the standalone system must be tagged and stored. Justification for retention will refer to the PPO investigation*

4.47. *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.*

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

4.48. *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, one labelled "Master Copy" and sealed in a signed evidence bag and the other labelled "Working Copy" and also 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 discs*
- *The full name of the person sealing the evidence bags*

4.49. *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*

4.50. The original footage on the hard drive of the standalone system will be tagged and stored; the risk assessment for retention whilst evidencing the need for internal Investigation.

Disclosing footage as part of an adjudication hearing

4.51. *Where material is required for adjudication purposes 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 disc*
- *The full name of the person sealing in the evidence bags*

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

4.53. At any hearing the expectation is that the Record of Hearing (DIS3 Form) has been fully completed with all relevant/detailed information relating to the incident from which the charge has fallen and that any evidence that has been referred to has been obtained. This may well include BWVC footage.

4.54. *BWVC footage forming part of the evidence in an adjudication must not be copied or sent to any third party. Arrangements must be made for the accused prisoners and legal advisors or representative 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, consideration must be given to the matter of the infringement of "personal rights" under data protection laws 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. This is outlined in Schedules 2 and 3 to the DPA.*

4.55. When viewing evidence of a prisoner's behaviour especially where the prisoner is believed to have taken an illicit or illegal 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. It is important to document this on the DIS3 form. Likewise it is important to record that a prisoner expressed a wish to view the footage.

4.56. The Adjudicator will notate the DIS3 Form to indicate, that digital footage has been shown and provide a brief outline of the contents. The prisoner will be given the opportunity to question the Reporting Officer (RO) regardless of any plea of guilt and any absence of the RO. Should the prisoner wish to question the RO then the hearing will be adjourned to facilitate that and the Adjudicator will notate the DIS3 to that affect.

4.57. *Once the hearing is concluded to a final outcome the disc must be destroyed and the evidence log noted accordingly. The original footage on the system however must be retained until it is confirmed that all potential uses of it, including appeal mechanisms have been completed and this would conform to guidance contained in PSI 35/2014 on the retention and disposal of adjudication records*.

4.58. Further information on adjudication procedures can be found in PSI 47/2011 Prisoner Discipline Procedures.

Third party requests – Subject Access Requests

4.59. Section 7 of the Data Protection Act 1998 gives individuals the right of access to their own personal data usually referred to as Subject Access Request (SAR). It provides that an individual is entitled to be informed if personal data relating to them is being processed a description of the personal data of which they are the data subject the purpose for which it is being processed and the recipients to whom this may be disclosed. They are also entitled to have communicated to them in an intelligible form the information held. Such information requests could include material obtained through the use of BWVC and should be handled in accordance with establishment policies, procedures and codes of practice.

4.60. 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 PSI 44/2014 DPA 1998, FOI 2000, EIR 2004.

4.61. *When releasing material under a SAR, care must be taken to review the footage and ensure that only the "subject's" image is revealed and the identity of staff, other prisoners and person(s) are obscured. Care must also be taken to ensure that no footage presenting a risk to security 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. Therefore, 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 PSI 44/2014, DPA 1998, FOI 2000, EIR 2004.*

5. Operational Scenarios

Spontaneous Use of Force (UoF)

5.1. 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.

5.2. In 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. In such circumstances users should explain why earlier recording was impracticable on the BWVC device and within their written statement.

5.3. *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*

5.4. *Users must justify their actions, perceptions and decisions as per normal within their written Use of Force statement. The writing of UoF statements will 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*.

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

5.6. *Where a full search occurs under restraint or following a Use of Force, BWVC may be used providing there is a justification to do so and users must set out the justification for use within the accompanying documents.*

Planned Use of Force (UoF)

5.7. *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.*

5.8. 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.*

5.9. 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 at a later date the rationale for the decision. *BWVC footage capturing UoF must be tagged and retained in line with UoF paperwork.*

Nights

5.10. 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 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.

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

5.11. BWVC are authorised to be used in all prisons which includes the use in Domestic/Legal visits area or the Visitors Centre.

5.12. *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.*

5.13. 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.

5.14. Managers may consider it prudent to retain any footage involving members of the public or visitors for the full 3 month period or set period thereafter with reasons set out in the justification assessment.

Incident Response – Medical Intervention

5.15. 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.

5.16. *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. Users will conduct a dynamic risk assessment and where no threat to the safety or security of others exists users must maintain audio capture but should consider non-intrusive capturing of the medical intervention. This may be the camera lens being directed at the head and shoulders of the staff involved, and occasional direct capture of the medical procedure, with an audio commentary of the events as they unfold.*

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

Routine Medical Treatments

5.18. 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.

6. System Management

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 "standby" 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 and burn footage to disc 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 3 month 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

Assigning Users

6.6. *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.*

6.7. No member of staff should be permitted to wear BWVC equipment unless they have carried out the required training and understand the principles of use.

Equipment Management

6.8. *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.*

6.9. *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*

6.10. *Any loss of BWVC equipment must be reported on IRS.*

6.11. *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. PSI 11/2012 Incident Reporting System Annex A/B/C refer.*

6.12. *The loss of BWVC equipment will also require reporting as a "Data Loss". PSI 24/2014 Information Assurance Policy Chapter 7 and Annex B provide guidance for this.*

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

6.14. 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.

6.15. 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. *If establishments choose not to use this inbuilt facility then a manual log must be kept and maintained for examination*.

System access

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

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

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

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

Documentation

6.20. *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*

6.21. *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*
- *Footage copied to disc*
- *Date disc to evidence log plus evidence bag reference number*

6.22. *Justification/decision log must capture the following information*

- *Date and reference number for justification assessment*
- *Retention decision*

6.23. *Evidence log must capture the following information*

- *Date and time*
- *Evidence bag number*
- *Brief description of evidence*
- *Audit trail of access/removal from safe*