

DEPARTMENT OF JUSTICE

**NAOMI LONG MLA
Minister of Justice
Block B, Castle Buildings
Stormont Estate
Belfast BT4 3SG**

**MR DOUG BEATTIE MLA
Northern Ireland Assembly
Parliament Buildings
Ballymiscaw
Stormont**


**25 May 2021
AQW 18614/17-22**

MR DOUG BEATTIE (Upper Bann) has asked:

To ask the Minister of Justice, pursuant to AQW 18168/17-22, to provide a copy of this policy.

ANSWER

A copy of the Northern Ireland Prison Service, Body Worn Video Camera Policy has been deposited in the Assembly Library.



NAOMI LONG MLA

Body Worn Video Camera Policy



April 2019

DOCUMENT INFORMATION

Owner	
Owner:	Director of Prisons
Author:	Head of Operational Support
Consultation	
	Governing Governors / Governors in Charge
	Prison Officers Association
	Prison Governors Association
Impact Assessments	
Equality Screening	April 2019
Data Protection Impact Assessment	April 2019
Approval	
Operational Management Board	12 December 2018
Version	
Version:	Final Version
Publication date:	April 2019
Implementation date:	April 2019
Review date:	As required

Introduction

Operational prison staff work with people in custody who have complex needs and risks, and who can display challenging behaviours. The Northern Ireland Prison Service (NIPS) places great emphasis on the safety of our staff and the safety of people in our custody, and continually examines the possibility of employing practicable measures to enhance safety and provide reassurance.

NIPS trialled Body Worn Video Cameras (BWVCs) in two establishments (Maghaberry Prison and Magilligan Prison) during 2016, as a potential enhancement to the existing suite of security equipment which staff have available for use. The objective of the trial period was to establish if the deployment of BWVCs could promote reassurance, modify behaviour, prevent harm and deter people in custody from committing offences against prison rules, as well as providing evidential quality video and audio recordings.

The trial period proved to be successful in establishing that BWVCs had a significant effect in the de-escalation of confrontational situations and also proved beneficial in providing recording of incidents for use in adjudications and court proceedings.

As a result of the findings during this trial period NIPS, supported by the Minister of Justice, extended the use of BWVCs to all three NIPS establishments. This policy and guidance provides advice for those involved in operating BWVC systems and operational staff who are deployed with a BWVC available for use.

NIPS Body Worn Video Camera Policy

1. Scope

1.1 The scope of this policy extends to the overt use of BWVCs in all areas of NIPS establishments. The scope of this policy and procedures covers BWVCs deployed for use by operational prison staff.

1.2 This policy must be considered as a minimum standard for the use of BWVC equipment and should be used as a basis for the development and implementation of establishment-specific operating procedures.

2. Justification for the Use of BWVC

2.1 The purpose of the deployment of BWVCs by NIPS is to:

- provide an additional tool for the de-escalation and resolution of conflict or confrontation;
- enhance the safety, security, good order and discipline of prison establishments and in other areas where BWVC is deployed within the scope of this policy;
- enhance the safety, security, wellbeing and welfare of prison staff, people in custody, visitors and the public;
- deter people in custody from committing criminal offences and/or offences against prison rules;
- promote transparency, trust and confidence between staff and people in custody;
- provide video and audio information to assist managers in the operation of prison establishments, for the oversight of incidents and their management and for the resolution of staff disciplinary investigations;
- provide evidential quality video and audio recordings for use in adjudications and court proceedings.

2.2 On this basis NIPS has taken the decision that the use of BWVCs as described in this policy is a proportionate and effective tool for operational prison staff. This policy takes into account the need for a proportionate response and the effect that the use of BWVCs may have on individuals.

3. Aims and Objectives

3.1 The aim of this policy is to ensure that all staff involved in the deployment, use or storage of Body Worn Video Camera recording equipment or material are fully aware of the systems and procedures required by the Northern Ireland Prison Service. All staff are bound by the policy, and supervisors in particular have a key role in ensuring that correct systems and procedures are followed at all times.

3.2 The specific objectives are to:

- define the requirements that must be met to comply with the Human Rights Act 1998, PACE, (NI), 1989 and the Data Protection Act, 2018.
- provide guidance for staff and managers in the use of downloading, handling and storage of subsequent materials involved in the operation of BWVC equipment;
- define the requirement for staff involved in the handling of equipment and / or material produced.

4. Principles Relating to the Processing of Personal Data

4.1 The data being processed by the BWVCs falls within the definition of law enforcement processing under section 31 of the Data Protection Act 2018 as being for “the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.

4.2 NIPS meets the requirement of the First Data Protection Principle as set out in section 35 of the Data Protection Act 2018 that the processing of personal data for

any of the law enforcement purposes must be lawful and fair. The processing is based on law and necessary for the performance of a task by a competent authority. NIPS is a competent authority as defined in section 30 of the Data Protection Act 2018.

4.3 As NIPS are processing sensitive processing in the use of BWVCs we must also meet the case specified in section 35(5) of the Data Protection Act 2018. This is met by the following:-

- The processing is strictly necessary for a law enforcement purpose;
- The processing meets the condition in schedule 8 in that the processing is necessary for a statutory purpose and for the administration of justice;
- An appropriate policy is in place.

5. Signage

5.1 All BWVCs deployed by NIPS will display clear signage when recording is taking place. All NIPS establishments where BWVCs are being operated will display signage showing that CCTV is in use.

6. Quality of Information

6.1 All BWVCs deployed by NIPS will produce images and sound recordings that are as clear as possible in order that they are effective for the purpose(s) for which they are intended. Staff responsible must also ensure that the CCTV system has the correct date and time display for evidential purposes.

7. Issue of BWVCs

7.1 The issue of BWVCs will be carried out from an appropriate designated area. This will be recorded in an issue / returns log. This log will be checked by the appropriate supervisor on a daily basis.

7.2 Operators must check that all equipment is functioning correctly. At the point of issue, equipment should be checked and confirmed correct. All details must be entered in the receipt / issue log.

7.3 BWVCs issued to staff must be deployed and worn. Local managers should ensure that staff comply with instructions for deployment and use.

7.4 All forms will be the responsibility of the appropriate supervisor and must be safely retained.

8. Activation of BWVCs

8.1 Local managers should take into account the presence and capabilities of staff equipped with BWVCs, and should deploy them to relevant areas as a matter of course.

8.2 Where there is no access to a camera or audio recording device, or staff are not available to operate them, and response or intervention is deemed to be necessary, it should not be delayed or postponed whilst awaiting arrival of staff and / or equipment, as this may well exacerbate an already serious situation.

8.3 The decision to activate a BWVC is the responsibility of staff, **not** a prisoner or visitor. Where possible, all aspects of incidents should be recorded, especially any threats, de-escalation, intervention or arrest phases, or where it is anticipated that an incident could occur (e.g. when unlocking a potentially disorderly or dangerous prisoner). Where staff feel it appropriate, they should deploy the equipment at an early stage in order to record as much of an incident as possible. A local Standard Operating Procedure about the activation of BWVCs must be issued, consistent with this policy.

8.4 Operators must always ensure that BWVC is only used as an overt audio or overt visual recording mechanism and is not intentionally used covertly. Where practicable a verbal warning should be given to persons involved in the incident that

audio / visual recording is being deployed. This may in itself act as a de-escalation strategy, e.g. “Everything you do and say is being video recorded”, “I am video recording you / this incident.” and “recordings may be used for the purposes of investigation, disciplinary proceedings, or criminal prosecution”.

8.5 It may be helpful, ONLY if circumstances permit and dependent on the type of the incident or event being filmed, for the operator 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.

8.6 Any footage or recording must generally be uninterrupted from the beginning of the incident until the end. 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 consult with their manager or a Governor when selective filming is used, and must ensure that explanation and justification is given for selective recording in the accompanying documents and/or written statement.

8.7 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 operators 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.

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

8.9 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 should be recommenced and a supporting explanation provided on film as soon as practicable in addition to being documented in any subsequent written statement.

8.10 Staff using BWVCs must ensure that the use of such equipment will not involve any unwarranted intrusion of privacy, and that it is fully justified in the circumstances of the incident or NIPS operation.

8.11 Whilst exceptional, it is accepted that there may be incidents where Body Worn Video Camera recording would not be appropriate. In these situations, the operator should balance the benefits of obtaining BWVC evidence against any relevant human rights considerations. It may be appropriate to pan away from gathering video footage, and only collect audio.

8.12 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 their use, for example in response to an incident where the safety or security of others is at risk. Users will be further aware of the sensitivity of using BWVC in places of worship where this may be viewed as disrespectful.

8.13 **Under no circumstances** should BWVC be directed into a cell where a prisoner is in a state of full undress except in extremis and when the necessity for using BWVC has been balanced with any relevant human rights considerations. If a search is taking place during an ongoing spontaneous incident where BWVC have been deployed, the camera can be turned away from the subject being searched so that video will not be recorded of the search, but all instruction and responses from the subject will be recorded as evidence.

8.14 On any occasion where the BWVC operator becomes aware that images of a prisoner in a state of undress have been recorded they should report this to the Security Manager who will ensure that the images will only be viewed by members of staff who are the same gender as the prisoner.

9. Cessation of Recording

9.1 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.

9.2 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

10. Return of Cameras

10.1 Equipment should be returned to the designated issue area **unless there is footage to be downloaded, in which case, the camera must be returned initially to the appropriately designated area.** The returned equipment will be recorded on the Return Form.

10.2 There is no requirement to download and save data immediately after each activation unless it will be required for investigation or other purposes. However all activations should be reported to a relevant supervising officer at the earliest opportunity.

10.3 All operators of equipment and those charged with downloading, processing and storing recordings should be aware of their responsibilities in accordance with NIPS policy and procedures and will be made aware of the sensitivity of handling images and recordings in accordance with the provisions of the Data Protection Act 1998 and other relevant legislation.

11. Viewing of BWVC Footage

11.1 In certain circumstances, it may be necessary to view incident footage. The operator, supervisor, or Security Staff may examine the footage to ascertain whether

or not there is an immediate need to identify offences against Prison Rule 38 or criminal offences, or to see if it contains evidential matter. Such viewings must be strictly limited to staff with reason to be present, and, if possible, should be supervised by an officer of at least Senior Officer Rank, who has had no direct involvement in the incident. In no circumstances must unauthorised personnel be allowed access to the recording. Local procedures should explain the procedures and authority required prior to viewing BWVC footage.

11.2 To prevent damage or loss of footage, all reasonable care must be exercised and the viewing should be on the system designated for that role. Any corrupted or damaged footage of an incident should be retained, even though images may not be recognisable when viewed.

11.3 When dealing with evidence available through BWVCs, it should be borne in mind that the operators may be further witnesses to any events recorded, therefore, consideration must be given to obtaining statements from operators in such circumstances as well as for purposes of continuity.

12. Handling and Processing of Information

Police and Criminal Evidence Act (NI) 1989

12.1 The handling of Video and Audio recording media and equipment will be subject to PACE procedures.

12.2 All recording equipment and any subsequent footage / audio retained will be itemised, serial numbered, and kept in appropriate storage to which access will be restricted.

12.3 Once a recording has been made, if there are no reasons to retain it, it will be kept for a maximum of 30 days, and then automatically deleted. If there is an incident which may be required for investigation or action, a unique identifier will be issued by the Security Department for the saved footage.

12.4 Any request for access to, or copies of, video or audio recordings will be made to Security Management Branch, NIPS Headquarters. All movement of copies or originals will be signed for and recorded.

Data Protection Act 2018

12.5 All Video and Audio recordings fall within the scope of the Data Protection Act 2018. The Information Commissioner's CCTV Code of Practice sets out the standards that apply to the collection, processing, storage and use of images relating to individuals.

12.6 In essence, recordings may be obtained, retained and processed for the prevention and detection of criminal activity, or the apprehension and prosecution of offenders. Recordings will also be used to assist with the investigation of incidents.

12.7 The use of BWVC equipment for these purposes must comply with the NIPS Information Asset Register. This covers the possible use of overt recording of prisoners, visitors, or any other persons falling within the responsibility of the Northern Ireland Prison Service.

12.8 Whilst in NIPS possession, it is essential that the integrity of recorded material is maintained. This is not only to safeguard their evidential value but also to comply with the law, which requires that measures will be taken to protect the rights of people and prevent unauthorised release, unlawful processing, accidental loss, damage or destruction of personal data.

12.9 This policy provides the guidance, advice, procedures and protocols required for the overt application, deployment and use of Body Worn Video Cameras by NIPS staff which is deemed to be a reasonable and proportionate use. It does not cover any covert use of video recording equipment, the use of which is subject to the terms of the Regulation of Investigatory Powers Act 2000.

13. Access to and disclosure of images to third parties

13.1 It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled. This will ensure that the rights of individuals are preserved, and also ensure that the continuity of evidence remains intact should the images be required for evidential purposes in a police enquiry.

13.2 Access to images that are displayed and recorded on CCTV systems is restricted to the appropriately trained staff and third parties, e.g. PSNI, Prisoner Ombudsman. Copies of recorded images should not be made without the prior approval of a Governor and the completion of the appropriate view/ release forms. Police officers obtaining a copy of the recorded images from any office will be required to provide a signed receipt which should be retained.

14. Subject access requests

14.1 The data being processed by the BWVCs falls within the definition of law enforcement processing under Section 31 of the Data Protection Act 2018. Section 45 of the Data Protection Act 2018 gives individuals the right to access their personal data and supplementary information subject to certain restrictions. Individuals who request access must be issued a subject access request form

14.2 An individual is entitled to the following information:-

- the purposes for processing and the legal basis we are relying on;
- the categories of personal data we are processing;
- recipients or categories of recipients we are disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);
- retention period, or our criteria for determining this;
- their rights to request rectification, erasure or restriction;
- their ability to raise a complaint with the Information Commissioner and the ICO's contact details; and

- the personal data we are processing (in writing) and any available information you have about the origin of the data.
- Any information supplied about the processing of personal data must be:
- concise, intelligible and easily accessible; and
- written in clear and plain language, adapting this to the needs of vulnerable persons, such as children.

14.3 Under no circumstances after a subject access request has been received, should a recording be deleted or overwritten until a decision has been made as to the validity or not of the subject access request.

Individual rights can be limited (in full or in part) if it is necessary and proportionate in order to:

- avoid obstructing an official or legal inquiry, investigation or procedure;
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- protect public security;
- protect national security; or
- protect the rights and freedoms of others.

Where requests are manifestly unfounded or excessive, NIPS can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond

14.4 A written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons where appropriate) within one calendar month of receipt of the enquiry. (Note: information should be provided promptly as information may be routinely deleted after 30 days).

14.5 You can restrict the amount of personal data you supply when it is necessary and proportionate to “protect the rights and freedoms of others.” If information

contains the personal data of an individual and that of third parties, you have to consider whether it is reasonable to disclose this information and whether this would adversely affect the rights and freedoms of others. You may need to consider pixelating images, and record any reasons for withholding such information from disclosure.

14.6 Detailed guidance on this and matters such as when to withhold images of third parties caught in images is included in the ICO CCTV Code of Practice.

Reporting Information Security Incidents, Breaches or Threats

14.7 It is the responsibility of all staff to report any perceived incidents, breaches or threats (whether observed or suspected) to business activities, systems or services to their line manager immediately. This includes BWVCs. Line managers must then report these suspected incidents or breaches to the NIPS Senior Information Asset Owner (SIAO) immediately. This will allow time for an assessment of the incident by the NIPS SIAO to consider whether the incident should be reported to the Information Commissioner's Office.

14.8 There is a mandatory requirement for NIPS to notify the ICO of serious breaches within 72 hours. Failure to report a breach can result in a fine of up to €10 million as well as the fine for the breach itself of up to €20 million.

14.9 In addition, where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the NIPS must inform the data subject of the breach without undue delay.

15. Documentation

15.1 Copies of all documentation and records relating to the CCTV system will be held on TRIM by the appropriate Security Department with appropriate access controls in place.

16. Training

16.1 Staff who are issued with a BWVC must have received training consistent with this policy. This training can be delivered by a suitably experienced and trained person at a prison establishment or by the Prison Service College.

17. Contact

17.1 Please contact your Security Department or HQ Security Information branch if you have any queries regarding this policy and guidance.