Newark and Sherwood District Council

BODY WORN VIDEO CAMERA POLICY

1.0 Document Version Control

	Last Modified	Last Modified By	Document Changes
1.1	09/04/2026	Information Governance for CIGG	Document first created
1.2	08/09/2026	SLT	Review for retention period and extension to cover contractors.

2.0 Document Contents Page

1.0 Document Version Control 2

2.0 Document Contents Page.....3

3.0 Introduction.....5

4.0 Body Worn Camera Policy 5

4.1 Purpose 5

4.2 Scope 6

4.3 Authorised Users and Training 6

4.4 Exclusions 7

5.0 General Principles 7

6.0 Legislation 8

7.0 Recording 8

8.0 Booking in Body Worn CCTV 9

8.1 9

8.2 9

8.3 9

9.0 Storage and viewing 9

9.1 9

9.2 9

9.3 9

9.4 9

9.5 9

9.6 10

9.7 Applications by individual data subjects 10

9.8 Access to and disclosure of images to third parties.....10

10.0 Policy Compliance.....10

11.0 Policy Approval.....11

3.0 Introduction

The Council uses overt surveillance systems for the purposes of public safety, crime prevention, detection and prosecution of offenders, monitoring council buildings and assets to protect the public, staff, elected members and visitors, and its property.

The Council fully recognises that the use of overt surveillance systems need to comply with a legal framework notably the General Data Protection Regulation (GDPR) and Data Protection Act 2018, and Article 8 of the European Convention on Human Rights (the right to respect private and family life).

This policy covers the use of body worn video camera systems and processing of images and information obtained from those systems and appropriate training. The policy takes into account guidance provided in the Surveillance Commissioner's, Surveillance Camera Code of Practice and the Information Commissioner's CCTV Code of Practice.

This policy does not apply to covert surveillance for investigation purposes which must only be carried out in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA). This policy should be read alongside the RIPA policy and the Council's Corporate Enforcement Policy.

This policy together with Councils' Data Protection Policy and operational guidance will support body worn camera users, owners and managers on the management, administration and operation of body worn camera systems.

The use of this policy will be referred to the Corporate Enforcement Group with an update provided to SLT every six months.

4.0 Body Worn Camera Policy

4.1 Purpose

The purpose of this Policy is to ensure that the operational use of Body Worn Video Cameras (BWV) is lawful, proportionate, legitimate and necessary; that it will be only used when deemed necessary for the purposes of violence reduction or evidence collection by trained staff in accordance with legislation, policy and procedures.

It sets out roles and responsibilities, provides staff with the correct procedures for collecting, downloading, processing and presenting video evidence, appropriate retention etc. This policy will ensure that the product of BWV devices is stored, retained, reproduced and disposed of appropriately.

The right to respect for private and family life is set out in Article 8 of the European Convention on Human Rights. The use of any form of surveillance may impact on an individual's privacy and rights under the Human Rights Act and data protection legislation (General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018).

BWV cameras are likely to be more intrusive than CCTV and deployable surveillance systems because of its mobility. BWV cameras have the ability to be switched on or off. Continuous recording

will require strong justification as it is likely to be excessive and cause a great deal of collateral intrusion.

The Council will prescribe guidance to officers covering the use of BWV Cameras where they are being used in situations where a higher level of privacy is expected, for example, in private dwellings. This guidance will also cover use with vulnerable individuals and sensitivities around religious or cultural beliefs and practices.

4.2 Scope

This policy applies to all staff that may use BWV and any associated hardware and software used for viewing and storing footage. Users of BWV include:

- Environmental Services: Environmental Protection Officers
- Public Protection: Community Protection Officers
- Housing: Housing and Estate Management
- Planning: Planning Enforcement Officers

This policy also applies to contractors acting on behalf of the Council and will be referenced within any new or extended contract.

A Business Unit deploying BWV will ensure that a Data Protection Impact Assessment (DPIA) is carried out and reviewed annually.

A Business Unit deploying BWV will ensure appropriate arrangements are in place for either allocating or booking out BWV devices to officers. Where a cloud-based solution is used the system will automatically log a device out to a designated officer when the device is removed from a docking station.

BWV should only be used:

- To reduce the number of incidents of aggressive behavior and abuse aimed at officers exercising their duties
- In the process of civil enforcement to ensure that it is accurate and transparent.
- To reduce protracted complaint investigations by providing impartial, accurate evidence.
- To support PACE interviews through the quality of evidence presented to alleged perpetrators.
- To evidence the good service of enforcement and advisory letters
- To gather evidence in investigations and for enforcement actions and proceedings.

4.3 Authorised Users and Training

Any user of BWV must be authorised by their Head of Service and must complete training before using the equipment. This will ensure that staff have the necessary skills and knowledge on the operational, technical and privacy requirements and fully understand the policies and procedures. This also ensures the reliability of staff having access to personal data
including images and information obtained by surveillance camera systems as required by

data protection legislation.

Business Units deploying BWV will develop training packages for their specific requirements and confirm with the Information Governance Team that these comply with data protection principles.

4.4 Exclusions

BWV will not be used for RIPA investigations unless the appropriate authorisations are in place.

5.0 General Principles

5.1 BWV devices are an overt method by which staff can obtain and secure evidence at the scene of incidents.

The use of BWV will be:

- Proportionate
- Legitimate
- Necessary
- Justifiable

5.2 These principles are intended to enable staff to comply with all legislative requirements. When used effectively BWV can capture best evidence, modify behaviour, prevent harm and deter people from committing offences and anti-social behaviour. The general principles of operation will include:

- BWV devices will be used overtly, fairly, within the law, and only for the purposes described in 3.2 of this policy
- Use of BWV will have regard to the principle that everyone has the right to respect for his or her private and family life and their home, and that the use of BWV must be proportionate, legitimate and necessary.
- Care will be taken to avoid recording third parties, particularly children or vulnerable adults, who may be present within a home environment, unless this is necessary for the purposes described in 4.2 of this policy.
- The public interest in the operation of the system will be recognised by ensuring the security and integrity of operational procedures and that data will be processed and managed in line with data protection requirements.

5.3 Data will:

- Be processed fairly, lawfully and in a transparent manner.
- Be adequate, relevant and limited to what is necessary.
- Not be kept for longer than is necessary.
- Be kept securely

6.0 Legislation

6.1 The integrity of any video data recorded will be considered in accordance with the following legislation:

- UK General Data Protection Regulation ('UK GDPR')
- Data Protection Act 2018 ('DPA 2018')
- Freedom of Information Act 2000
- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Regulation and Investigatory Powers Act 2000
- Home Office Surveillance Camera Code of Practice & Information Commissioners Code of Practice
- The Local Government Act 1972 (LGA 1972)
- Housing Act 2004, Section 239
- Safeguarding

6.2 Under UK GDPR and the Data Protection Act 2018 the legal basis for recording video data will normally be Public Task.

7.0 Recording

7.1 Recordings will not be made whilst performing normal or routine work. Recording must be as a result of something an officer happens to come across, incident or investigation specific. Officers must not indiscriminately record entire duties or patrols and must only use recording to capture video and audio of specific incidents or for particular investigations where there are no viable alternatives to capturing the evidence required. There may be occasions where routine inspections may require recording as part of an investigation or for officer's safety.

For the purposes of this policy an 'incident' is defined as:

- An engagement with a member of the public which in the opinion of the officer is confrontational, and where the officer believes they may be subject to physical or verbal abuse.
- The officer is approached by a member of the public in a manner perceived as aggressive or threatening.
- An observed or suspected breach of a legal requirement or licence condition

7.2 At the commencement of any recording the officer should make an announcement (where possible) to indicate why recording has been activated.

The purpose of making a verbal announcement is to:

- alert the person to the recording taking place, or
- allow a member of the public to modify any unacceptable confrontational or
- allow a member of the public to modify aggressive and threatening behaviour, and/or

- To describe the purpose of activating the device

7.3 If, at any time during an incident the officer considers that the use of body worn cameras is likely to inflame a confrontational situation, the officer may use discretion to stop recording, disengage from further discussion and withdraw from the incident.

7.4 A specific form of words to be used in any warning to a member of the public has not been prescribed, but officers should use straightforward speech that can be easily understood by those present such as 'I am wearing a body worn camera and I am now recording'.

7.5 Incident Reports should be completed where required and submitted to the Line Manager.

8.0 Booking in Body Worn CCTV

8.1 Officers shall return BWV devices to the secure storage location as soon as is practicable. Units must never be taken home or left in open accessible locations such as on desks or in vehicles.

8.2 Officers should download any footage to the appropriate network area as soon as possible. Any CCTV footage required for evidential purposes must be correctly bookmarked by the officer.

8.3 Officers should report any BWV device faults as soon as possible.

9.0 Storage and viewing

9.1 All information recorded will be encrypted so that only authorised personnel can view it. All recordings are automatically overwritten after 28 days unless downloaded for the purposes defined below.

9.2 Downloaded recordings will be stored on the council's network or approved cloud-based system. The recordings will only be accessible by authorised personnel.

9.3 If evidence for investigations and or proceedings is downloaded, the following will apply:

Recordings for summary only offences will be deleted after six months from the date of the offence or the date on which the officer is satisfied an offence has occurred, if the matter has not been issued at Court.

Evidential recordings for other proceedings issued by or issued against the Council will be retained for six years following the final determination by the Courts.

9.4 A record or audit trail will be kept detailing how any information required by, or used as evidence in court by the Police or other statutory body has been handled.

9.5. Any evidential data will be deleted once it is no longer required. A record or audit trail of this process will also be retained.

9.6 The recording will only be viewed by authorised personnel, and any viewings will be logged so that there is an audit trail. The following situations will apply:

- **a.** An officer has reported an aggressive/abusive incident which needs to be investigated further or reported to the Police.
- **b.** A complaint has been received concerning the manner in which a PCN, FPN, CPW or CPN or any other notice has been issued, or the behaviour of an Officer needs to be investigated.
- **c.** A member of the public has requested a copy of the recording that was made of them. You will be informed by the Information Governance Team if this is the case.
- **d.** Evidence has been requested by the Police or other statutory agency or is required as evidence in court.
- **e.** Where the footage may assist in upholding a notice served or any other investigation or court proceedings.
- **f.** Other situations where it is authorised by a Director of the Council.

9.7 Applications by individual data subjects

Individuals can request images and information about themselves through a subject access request under GDPR. The Council has a team which handles requests. The Council publishes information on its website on how to make a request and also have specific forms to request BWV footage.

Data subjects' rights and the Council's processes for handling requests are covered in the corporate data protection training which is mandatory for all new employees with refresher training provided every two years.

The disclosure of images to data subjects is done securely to ensure that they are only seen by the intended recipient. Consideration is also given to whether images of other individuals need to be obscured to prevent unwarranted identification.

9.8 Access to and disclosure of images to third parties

Disclosure of images or information may be appropriate where there are relevant exemptions which allow it, provided that the requirements of the Act are met, or where permitted by other legislation.

These exemptions include where non-disclosure would be likely to prejudice the prevention and detection of crime, and for legal proceedings purposes. There may be other limited occasions when disclosure of images to another third party, such as a person whose property has been damaged, may be appropriate. The Council will consider such requests with care and in accordance with data protection legislation.

The Council has discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once the Council has disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image. The Council will include in its operational guidance supporting this policy, arrangements for secure disclosures to third parties.

10.0 Policy Compliance

An employee found to have deliberately contravened this policy or caught jeopardising the security of data which is the property of the Council may be subject to disciplinary action, up to and including termination of employment and where necessary legal action may be taken, in accordance with the Council's Human Resources policies and procedures.

11.0 Policy Approval

This policy is approved by, CIGG, SLT, Cabinet and is fully supported by the Council.