Northern Ireland Ambulance Service
Health and Social Care Trust

Title:	**Body Worn Video (BWV) Policy**		
Author(s):	Sheridan Easter, Fire & Security Advisor Katrina Keating, Risk Manager		
Ownership:	Maxine Paterson, Director of Planning, Performance & Corporate Services		
Date of SMT Approval:	7th June 2022	**Date of ARAC Approval:**	23rd June 2022
Operational Date:	23rd June 2022	**Review Date:**	June 2023
Version No:	1.0	**Supercedes:**	N/A
Key Words:	Assault, aggression, violence, safety, CCTV, body worn video cameras (BWV), images, evidence, data protection, GDPR, Freedom of Information, Subject Access Request, privacy impact assessment, staff attacks, incidents, legitimate interest assessment.		
Links to Other Policies / Procedures:	Security Policy, Management of Aggression Policy & Procedures, Corporate Risk Management Policy and Strategy, Health and Safety Policy and Procedures, Risk Assessment Procedure, Information Governance Policies and Procedures, PPI Strategy, Learning From Serious Adverse Incidents (SAIs) Procedure, Incident Reporting Procedure.		

Version Control:			
Date:	**Version:**	**Author:**	**Comments:**
June 2022	1.0	Risk Manager	New Policy

1.0 INTRODUCTION:

This policy establishes the legal basis and provides guidance for the use of body worn video (BWV) by the Northern Ireland Ambulance Service Health and Social Care Trust.

1.1 Background:

The Northern Ireland Ambulance Service Health and Social Care Trust (NIAS) is committed to ensuring, so far as is reasonably practicable, the health, safety and welfare of its staff, service users and anyone else who may be affected by its activities.

The Trust must comply with the minimum legal requirements with regards to health and safety, and wherever possible shall exceed them. Under the Health and Safety at Work (NI) Order 1978, and the Management of Health and Safety Work (NI) Regulations 2000, the Trust is required to assess risk and maintain an environment that is, so far as is reasonably practicable, safe and without risks to health.

It is an unfortunate fact that whilst caring for others, NIAS staff are exposed to violence and aggression (average of 13 incidents per week 2021/22). The Trust aims to reduce this risk to staff by the implementation of body worn video (BWV) incorporating audio. The use of BWV is on the increase. The technology is now being utilised by a number of Health Trusts in Northern Ireland, the majority of ambulance services in England and many public bodies such as the Police Service of Northern Ireland (PSNI), local authorities and the Department of Agriculture, all in an effort to enhance and improve staff security.

A strategic aim of the Trust is to improve staff health and wellbeing and reduce risk wherever possible. The introduction of BWV is designed to reduce risk to staff with an associated reduction in sickness absence.

1.2 Purpose:

The purpose of this policy is to ensure that the operational use of BWV is proportionate, legitimate and necessary; that it will be only used when deemed necessary for the purposes of violence reduction, 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.

1.3 Objectives:

This policy seeks to ensure the following:

- Compliance with the appropriate legislation and guidance including requirements around privacy, the Data Protection and Freedom of Information legislation.
- A reduction in the risk of violence and aggression towards staff as BWV devices should act as a deterrent (clearly demonstrating that actions may be recorded).
- That staff are trained and have detailed guidance on the collection, downloading, processing, presentation and retention of video / audio evidence.
- That BWV devices are used correctly to maximise their benefit.

- The provision of compelling, high-quality video / audio footage thereby supporting the likelihood of the successful identification, apprehension and prosecution of offenders in relation to violence and aggression towards staff.
- Safeguarding of public assets.

2.0 SCOPE:

This policy applies to all staff who use BWV devices and / or the associated software along with the subsequent management of any images obtained.

3.0 ROLES AND RESPONSIBILITIES:

3.1 The Chief Executive is responsible for:

- Ensuring that there are suitable and sufficient arrangements in place for the management of BWV within the Trust, including the necessary resources, monitoring processes and oversight.
- Ensuring the full and effective implementation of this Policy, and satisfying Trust Board of the same.
- Ensuring there are suitable arrangements in place for the review and audit of this policy document to ensure that the policy remains fit for purpose and that full policy compliance is achieved.

3.2 The Director of Planning, Performance & Corporate Services is responsible for:

- Providing the Chief Executive and Trust Board with information and assurance pertaining to the management of BWV within the Trust.
- Ensuring that NIAS has a robust system and structure in place for the use of BWV.

3.3 Directors & Assistant Directors are responsible for:

- Implementing this Policy and any associated guidance.
- Ensuring arrangements are in place for monitoring and compliance with this Policy.
- Ensuring that there are suitable resources available for the implementation of this Policy.
- Informing the Risk Management Team where there is a significant change in corporate structure or operational practices.
- Ensuring all employees are made aware of this policy and the requirement for their professional conduct at all times during employment.

3.4 Ambulance Service Area Managers (ASAMs) & Station Officers (SOs):

- Implementation of this policy at divisional level.
- Ensuring all staff are aware of the contents of this policy.
- Ensuring all person under within their divisions / teams comply with this policy.
- Ensuring that all incidents are reported and managed via the necessary means and that the Trusts Incident Reporting Procedures are complied with.
- Ensuring that all staff comply with this policy, any concerns are address, and any deviations from this policy are investigated and addressed.

- Escalate any concerns that cannot be addressed at a local level to the Risk Management Team.

3.5 The Risk Management Team is responsible for:

- Information Asset owner for the Trust's BWV systems (Risk Manager).
- The development of suitable policies and procedures compliant with legislation and guidance relating to the use of BWV.
- Developing and implementing a training strategy for all users of BWV, and ensuring any training is recorded in line with Trust procedures.
- Carrying out and regularly reviewing Data Privacy Impact Assessment(s) (DPIA) in partnership with the Information Team with regards to the use of BWV.
- Procurement of BWV devices and associated hardware.
- Supporting line managers with the relevant training in the use of BWV devices.
- Acting as the single point of contact between NIAS and external parties such as HSENI and PSNI.
- Supporting line managers with the investigation of any incidents, issues or claims pertaining to images and information captured on BWV devices.
- Provide assistance and advice on the use of captured images following incidents.
- Ensuring BWV systems have maintenance/management contracts in place.
- Ensure that adequate signage is in place indicating use of BWV (camera stickers etc.).

- In partnership with the Information Team, ensure that regular audits are carried out to ensure compliance with legislation/policy.

3.6 The Data Protection Officer (DPO) is responsible for:

- Ensuring that all the BWV systems are registered with the ICO.
- Ensuring that systems are managed by The Digital System Administrator.
- Delegate the duties of data controller to the DEMS Manager for each upload point.
- Advise appropriate staff on all data protection issues relating to BWV devices.
- Provide advice to authorising senior managers to enable them to make informed decisions on authorisation.
- Take part in the planning and authorisation process for all new BWV devices and systems.

- Liaise with PSNI / local authorities etc. for release of data / information.
- Ensuring that the relevant privacy notices are available and up to date.

3.7 All Staff using BWV are responsible for:

- Reporting of any incidents of significance in a timely manner.
- Using the BWV device within the remit of this policy and their training.
- Complying with Trust information security policies and procedures. Recorded data must not be used for any purpose other than that which is legitimate under the relevant policies and procedures.
- Ensuring they use their own dynamic risk assessment to determine if a recording of the situation is justified and warranted.
- Not to misuse or abuse the supplied BWV devices in anyway.
- Taking personal responsibility for the security of the BWV device.
- Reporting any concerns regarding the equipment or use.
- Ensuring the BWV devices are signed out at the start of each shift, and subsequently left back to the docking station at the end of same, on charge and in an operational condition.
- The mandatory use of BWV as one of a number of tools provided staff safety.
- Only using BWV whilst on duty / in uniform.
- Ensuring footage from BWV devices is not recorded using mobile cameras or video recorders. This is not an acceptable process.
- Noting that the use of BWV does not replace the need to write statements or complete records of incidents etc.
- Acting in a professional manner at all times and taking personal responsibility for their actions.
- Not discouraging the use of BWV to crew mates.
- Not interfering with colleagues dynamic decisions with regards to when to record. Every individual is autonomous as to when they wish to activate BWV. Colleagues must not dictate to other staff as to when their cameras should / shouldn't be activated.

3.8 The Information Assurance Group:

- Oversight of this policy and its impact within the organisation.
- Ensuring the contents of this policy do not directly affect or have a conflict of interests with any other policy or procedure within the trust.
- Consultation with any other agency or Trade Union representatives on the content of this policy.
- Agree to the final sign off and implementation of this policy within the Trust.
- Regular audit of processes and review of associated data.
- Consideration of the requirement to develop an 'External Stakeholder Advisory Panel' (2/3 times per year).

4.0 KEY PRINCIPLES:

4.1 Body Worn Video (BWV):

Is a wearable audio and video recording system used to record events in which the wearer is involved. It is typically worn on the torso of the member of staff and on the uniform using a variety of carriage solutions.

The equipment is usually implemented to meet a specific need (violence prevention and reduction in NIAS). There are multiple manufacturers and suppliers of equipment and associated digital evidence management software (DEMS).

4.2 Surveillance Camera Systems:

Has the meaning given by Section 29(6) of the 2012 Protection of Freedoms Act and is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c)1.

4.3 Overt Surveillance:

BWV devices are 'overt' meaning that they are visible and obvious. Overt means any use of surveillance for which authority does not fall under the Regulation and Investigatory Powers Act 2000 (Amendment) Order (NI) also known as RIPA. **NIAS Body Worn Video Cameras will not be used for covert recording under any circumstances**.

4.4 Body Worn Video (BWV) – Privacy Impact Assessment:

BWV devices can be intrusive to personal privacy and the decision to implement and use BWV devices within the Trust has been informed by a thorough assessment known as a 'Data Protection Impact Assessment' or DPIA. This DPIA was led by the Risk Management Team and Information Team and has considered the following:

- Justification for implementation and use of BWV.
- Benefits is to be gained from its use now and in the future.
- Responsibility for the system and images under data protection requirements.
- Purpose of the system, and what problems it is going to address.
- Project scope and potential for project creep and addressing these issues.
- Minimising intrusion for those who are not intended to be filmed.
- System authorisation.
- System procured, installed, used/maintained in accordance with requirements.

4.5 General Principles:

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.

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 for which it was established.
- Operating BWV with due 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 BWV must be proportionate, legitimate and necessary.
- 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. 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.

4.6 Information Commissioner's (ICO) Data Protection Register:

The Trust is appropriately registered with the Information Commissioner's Office, for the collection and processing of data, registration number Z5545963

4.7 Issuing of BWV Devices & Docking Stations:

- BWV devices will be held centrally by the Risk Management Team and allocated to each division / station as necessary.
- Each device will be uniquely identifiable by a serial number. This will ensure all devices are accounted for and their location identified at all times. This information will be stored centrally in a secure electronic format, accessible only by authorised personnel.
- Docking stations will be allocated to each division/station as necessary and proportional to the number of BWV devices issued to same.
- Docking stations will be stored in a secure location accessible only by authorised ambulance personnel. All docking stations will be uniquely identifiable by serial number ensuring accountability and location of each station at all times.
- Spare BWV devices and docking stations will be held centrally in the event of replacements being required due to loss, theft, damage or malfunction of operational units.
- If a replacement device or docking station is required, Risk Management Team should be contacted detailing the reason for exchange. The defective device MUST be handed back to the responsible person in order to secure a replacement device.
- Only appropriately trained staff will be authorised to receive and use BWV.

4.8 Training In The Use of BWV Devices / Docking Stations:

- All operational staff who have been identified as potential users for BWV devices will be trained in how to use the devices.

- The training will include:
    - Applicable legislation and legal requirements of using BWV devices in a public area, privacy, data protection, information governance etc.
    - Framework and reasons for implementation of devices throughout the Trust.
    - How to mount the device on the body.
    - How to operate the device, turning on/off and various functions.
    - When to operate the recording function and the parameters of permitted use.
    - Permissions of use, how to alert the public recording is about to commence and reasons why.
    - Maintenance and charging of the device.
    - How to dock the device for information and data upload/transfer.
    - The timeframe for uploading of information and data.
    - How the information and data is stored and erased from the devices.
    - Implications for misuse.
- All personnel must attend a full training session prior to operating the BWV device in an operational environment.
- All personnel must sign to acknowledge they have been trained in the use of BWV devices and understand their legal responsibilities in its use.
- Records of this training will be held centrally for audit and accountability purposes.

4.9 Access To BWV Devices:

- All staff must receive training in all aspects of the BWV devices and have read and understood the policy and procedures for their use.
- Staff are required to sign in agreement with the terms and conditions of use as detailed within this policy and confirm training on the devices (form BWV1 – Appendix 1).
- On completion of training, each member of staff will be allocated a unique ID card, which will be used to access the radio frequency identification (RFID) reader on the BWV Digital Evidence Management System (DEMS) which will automatically assign a specific BWV device to them.
- The DEMS retains an audit trial for each BWV device, recording who it has been assigned to and when the device was returned to the docking station.

4.10 Operational Use of BWV Devices:

- Each device must remain allocated to the staff member for the full duration of the shift and must not be shared with other staff members during this time.
- The device must **only be operated by the staff member if there is a threat of violence and aggression, or actual violence or aggression**, and the situation warrants the activation of the device to start recording.
- Activation of the BWV device and recording of an incident is entirely the individual user's decision and each circumstance will require a dynamic risk assessment to justify the use of the device.
- Staff do not require the consent of the service user or other individual/s to begin recording as staff safety is paramount. The staff member must however make the individual/s about to be recorded aware of this by verbal means. At the

commencement of any recording the user should, where practicable, make a verbal announcement to indicate why the recording has been activated, such as -

I am wearing and using a body worn video camera which is recording both video and sound'.

- If recording has commenced prior to engaging with an individual, they should be informed that recording is on-going, as soon as is reasonably practicable.
- Operators should, when practicable, inform any persons engaging with them, i.e. police, other health and social care staff etc., that they are using their body worn cameras.
- Signage on the cameras will also alert the individuals that recording of images and voice is about to begin.
- It is important to record as much of an incident as possible; therefore recording should begin at the earliest opportunity from the start of an incident.
- In so far as is practicable, users should restrict recording to areas and persons necessary in order to obtain evidence relevant to the incident and should attempt to minimise collateral intrusion for those not involved. Every effort should be made to ensure that personal information of victims or witnesses is not inadvertently recorded on BWV.
- Staff should be aware of high sensitivity areas such as hospitals, prisons, police stations etc. and avoid recording unnecessarily.
- The recording must cease as soon as reasonably practicable, the incident has been dealt with or de-escalated to a point the staff member, using their own dynamic risk assessment, no longer feels under threat and the incident has come to a conclusion.
- Staff should be cognisant that if they fail to operate the BWV device during an incident of a significant nature, further explanation as to why they did not record the incident may be required.
- Staff must not use the BWV device for any other reason than to record an incident of violence and aggression or what they believe will escalate to an incident of significance.
- Any accidental or unneeded recording of footage should be reported to the Risk Management Team.
- Staff must ensure the device remains with them at all times during their shift.
- Staff must make all reasonable efforts to ensure the device is kept secure, clean and in an operational condition.
- Any losses, defects or malfunctions should be reported to the Risk Management Team.
- When the staff members shift finishes they must place their BWV device in the docking station to ensure it remains charged and ready for operational use.
- There may be occasions where footage or information captured for the prevention and reduction of violence is required to be used for other processes for example employment processes. This will be strictly managed on a case by case basis by the Information Team. This information may only be used to support either parties' claims as evidence to the claim being made or disputed.

4.11 Objections & Requests For / Against Recording:

There may be occasions where a person objects to being recorded. BWV wearers may record overt video and audio without consent if this recording is for violence prevention and reduction purposes as outlined in the Trusts Privacy Notice.

The decision to continue recording should remain with the BWV wearer, who should consider the objections made by the person in respect of the recording. The presumption should be, however, that recording should continue unless the objection(s) made overrides the need to record an evidential encounter. If the BWV wearer decides to continue recording despite objections, they should record the rationale in DATIX as to why they have decided to do so. They should also take steps to advise the individual as to the following:

- The reason for the recording taking place (violence prevention and reduction).
- Material recorded on BWVs will only be retained for a maximum of 31 days, unless required for evidential purposes.
- Footage is subject to the data protection legislation and can be applied for on request in writing.
- Any material is restricted and will only be disclosed to 3rd parties in accordance with the law.
- The recording is being made in order to act as a corroboration of the encounter and thus can be used to back up the accounts of each party.

Equally, BWV wearers may encounter members of the public who specifically request that any encounter or interaction is recorded, even if the BWV wearer does not feel that there is any evidential reason to do so. Unless there are clear reasons to do otherwise, the BWV wearer should record such an encounter, but should remind the person requesting the recording that, unless there is an evidential reason to retain the footage, it will automatically be retained for a maximum of 31 days and deleted thereafter.

4.12 Docking of BWV Device & Upload / Transfer of Information:

- All BWV devices must be returned to a docking station immediately after operational use, where any recorded footage will be automatically downloaded to the secure server. The data will then be deleted from the device, which will be charged for its next use.
- The information will be encrypted and cannot be accessed by the BWV device user.
- All recorded footage will be held on the secure server for 31 days before being automatically deleted.
- Recorded footage which is required for evidential purposes must be marked as an incident and burned to disc by the DEMS Administrator within 31 days. For prosecution cases four discs will be required; one master copy and three working copies. It is the responsibility of the Trust Investigating Officer to ensure that any footage required for evidential purposes is burned to disc before the expiry of the 31 day period.
- Details of the incident must then be recorded on DATIX referencing the BWV device serial number and docking station serial number.

- The BWV device must be swapped for a replacement device and allowed sufficient time to finish the upload and to recharge the battery.
- No BWV device should be used if it still contains data or information from a previous incident.

4.13 Digital Evidence Management System (DEMS):

The Digital Evidence Management System (DEMS) is the encrypted software that allows NIAS staff access to the data captured on the BWV devices. The system is configured so that it will recognise BWV devices from any NIAS location. This will allow authorised staff to view footage from any device and from any location after the device has been docked.

Authorised staff will only be able to access and use the DEMS once they have been trained and setup with a login / password. NIAS authorised staff will have roles assigned to them when users are generated. The following roles/access roles have been generated;

- DEMS System Administrator – full access to the DEMS i.e. view all videos, incident bookmark, burn incidents to disc, setup new users, password resets, amend permissions, removed incidents, delete files (full access).
- DEMS Manager – management roles are setup to have access to all videos and mark incidents. They must notify the Administrator if they require an incident to be burned to disc.
- DEMS User – staff will only be able to view data they have captured. If a user requires recorded footage to be marked as an incident they should report via Datix and contact the Risk Management Team.

4.14 Loss / Theft of BWV Device:

- In the unlikely event of a device being stolen, the information cannot be accessed or viewed by any other person due to the encryption method used to record the information.
- The Risk Management Team, Information Governance and line management must be informed immediately in the event of a theft of a device, so swift action can be taken.
- In the event of a loss of a BWV device all reasonable attempts must be made to trace the device by the staff member. A DATIX must be completed immediately via personal issue tablet or on return to site / station listing the Risk Manager as the line manager and detailing the movement of the staff member and approximate time and location of the loss.
- A report to the PSNI must also be filed stating the loss / theft of the device by the staff member and the Risk Management Team advised of the PSNI Incident Number.

4.15 Security & Handling of Information Captured:

Unlike standard CCTV installations, BWV devices do not record continuously. Recording only commences once manually activated by the individual wearing the device (as a result of violence / aggression and / or threat of violence or

aggression). The device does however capture the previous 30 seconds of video – with no audio recording, as part of the recording.

- Any non-evidential data is automatically destroyed within 31 days.
- Any data / information recorded / stored will only be kept for as long as necessary to allow for all investigations, legal proceedings and convictions to be finalised and in line with the Trusts retention and disposal arrangements.
- Recorded material will be stored in a way that maintains the integrity of the information and ensures the rights of individuals recorded by BWV devices are protected and that the information can be used as evidence in court.
- The information will be stored in a secure location with restricted access and fully encrypted.
- Images and information will only be accessible by authorised staff.
- Recorded images will only be viewed in a restricted area, such as a designated secure office. This viewing must be carried out under the direct supervision of an authorised officer.
- Where BWV recordings are required for evidential purposes in legal proceedings, they will be properly processed following consultation with the Information Team and DEMS Administrator.
- Information and data will be recorded and stored, in a recognisable and useable format. This will allow ease of transfer if required, to other agencies. Such formats will be of digital standard.
- The recording will be placed in a sealed envelope which is signed, dated and then stored securely until the investigation is complete.
- Most requests from the Police can be dealt with during normal working hours, although there may be occasions where urgent access is sought, particularly when dealing with serious crimes. These requests will be dealt with accordingly.
- The Police and others legitimately requesting access to images should only be given copies of the original data. Copies should be made onto portable media, such as write-only DVDs and handed over against a signature. Images should not be sent by email or other networked systems. The Police will usually provide their own portable media storage devices.
- There may be very rare occasions when the Police require the original recording device, or the hard disk drives from the device. This may be necessary to safeguard forensic data following a serious incident. Release of recording devices or hard disk drives will be actioned by the Information Team in line with existing procedures.
- No secondary recording of images and data is permitted under any circumstances (phone recording a monitor for example).
- Any person found recording of information or data on a secondary device will be referred to the appropriate enforcing authority for investigation.
- Misuse of BWV devices and equipment, unauthorised processing of data may be a criminal offence under the Data Protection Act.

4.16 <u>Disclosure of Information:</u>

- Disclosure of information from any of the Trusts BWV devices will be controlled and consistent with the purpose(s) for which the scheme was established.

- The date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) will be recorded accordingly.
- Each recording will be viewed and if necessary, images of persons not directly involved in the incident will be obscured to protect their identity and comply with data protection requirements.
- When disclosing images of individuals, consideration will be given to whether or not obscuring of identifying features is necessary. Whether or not it is necessary to obscure will depend on the nature and context of the footage that is being considered for disclosure.
- Judgements about disclosure should be made by the Information Team. They have 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 information has been to another body, such as the police, they become the data controller for the copy they hold. It is their responsibility to comply with the Data Protection Act (DPA) and UK GDPR in relation to any further disclosures.
- The method of disclosing information will be secure to ensure they are only seen by the intended recipient/s.
- Under no circumstances should copies of non-evidential material be burned to disc.

4.17 Subject Access Requests (SARs):

Data Protection Legislation provides individuals with a number of rights in relation to the processing of their personal data. One of these rights is the right to be provided with a copy of the information constituting the personal data held about them, in appropriate cases.

- Individuals whose information is recorded have a right to view this information and unless they agree otherwise, to be provided with a copy of that information. This must be provided promptly and within no longer than one month of receiving a request.
- Those who request access must provide details which allow the Trust to identify them as the subject of the information, and also to locate the information on the system.
- All individual subject requests will be logged and suitable records maintained.
- The Information Team will manage any Subject Access Request disclosures.
- A clearly documented process for these requests will consider the following:
    - The details required to find the information. Is it made clear whether an individual will need to supply a photograph of themselves or a description of what they were wearing at the time they believe they were caught on the recording, to aid identification.
    - If details of the date, time and location are required.
    - The information will be provided to the applicant free of charge.
    - Has the information been clearly labelled to assist in the identification process.
    - How the individual will be provided with a copy of the information.
- As previously mentioned, if the information or images captured contains third party images that are unrelated to the initial request, these images should be obscured under the Data Protection Act (DPA) and UK GDPR.

Video files can be accessed by those employees who record them and are reminded to act in accordance with the 'Confidentiality Code of Conduct'. Video files will only be downloaded and provided on request to support the progress of employment processes / investigations and under Trust Policy / procedures, and can only be provided to employees with a legitimate business need (including Trade Unions), who should act in accordance with the 'Confidentiality Code of Conduct'. NOTE files will only be shared within the HSC domain/secure network.

4.18 Freedom of Information (FOI):

- All requests for information under Freedom of Information will be dealt with on a case by case basis.
- Requestors may only ask for information regarding the general operation of the BWV devices, the allocation of them, or the costs of purchasing, using and maintaining them. If individuals are capable of being identified from the relevant recording, then it is personal information being held about the individual concerned. It is generally unlikely that this information can be disclosed in response to an FOI request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the Data Protection Act (DPA) and UK GDPR.
- However, consideration can be made of the expectations of the individuals involved, what the information considered for disclosure would reveal and the legitimate public interest in the information when deciding on whether disclosure is appropriate.
- Even where footage is exempt from FOIA/FOISA it may be lawful to provide it on a case-by-case basis without breaching the Data Protection Act (DPA) and UK GDPR.

4.19 Complaints:

- Formal complaints received in relation to any issue pertaining to the use of BWV will be managed through the Trust's complaints process with assistance from the local managers, and advice from the Information Team and Risk Management Team.
- Complaints received about processing under the Data Protection Act will be dealt with by the Information Team.
- Where these cannot be resolved, the individual has the right to escalate the complaint to the office of the Information Commissioner (ICO)

5.0 IMPLEMENTATION OF POLICY:

5.1 Dissemination:

With regards to dissemination this procedure will be:

- Issued to all Board Members, Chair, Non-Executive Directors, Chief Executive, Directors and Assistant Directors.
- Disseminated to the required staff by Assistant Directors.

- Made available on the Internet and SharePoint so that all employees and members of the public / stakeholders can easily have access.
- Discussed during Corporate Induction and training on the use of BWV.

5.2 Resources:

Information contained within this policy will be made available to new employees at the commencement of employment, at employee induction programmes, and via information leaflets.

5.3 Exceptions:

Non-operational staff, office based staff and non-patient facing roles who are not required to wear BWV devices.

6.0 MONITORING:

It is the responsibility of the Information Assurance Group to monitor the implementation of and assess the level of compliance with this procedure.

Random audit checks by the Information Team and / or the Risk Management Department will be regularly undertaken to ensure compliance with this policy and the current legislation. This will be in the form of randomised docking of devices and ensuring that no irrelevant or unnecessary data or information has been recorded.

7.0 EVIDENCE BASE/REFERENCES:

The above objectives will be met ensuring full compliance with the following legislation, policy and guidance:

- Health and Safety at Work (NI) Order 1978 and associated Regulations.
- UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018.
- Northern Ireland Act 1998.
- Equality Act 2010.
- 2012 Protection of Freedoms Act.
- Regulation and Investigatory Powers Act 2000 (Amendment) Order (NI).
- The Freedom of Information Act, 2000.
- Human Rights Act 1998.
- Surveillance Camera Code of Practice 2013.
- Technical Guidance for Body Worn Devices, Home Office, July 2018.
- Encryption Guidance, Information Commissioner's Office.
- CCTV Code of Practice, Information Commissioner's Office, May 2014.
- Guide to Law Enforcement Processing (Part 3 of the DP Act 2018).
- Information Commissioner's Office, 2018.
- Surveillance Camera Code of Practice, Surveillance Camera Commissioner, June 2013.
- The Police and Criminal Evidence (NI) Order 1989.

8.0 CONSULTATION PROCESS:

This procedure has been developed by the Fire & Security Advisor and the Risk Manager. Consultation took place with the Head of Informatics, Human Resources, Equality & PPI, Trade Unions, Senior Managers, Assistant Directors and Directors within the organisation. The final content of the document was agreed by the Violence Prevention & Reduction Group, Health and Safety Committee and Information Assurance Group, before SMT approval. The Policy was subsequently agreed by the Audit & Risk Committee.

9.0 APPENDICES:

Appendix 1 – Confirmation of Training and Terms of Use

10.0 EQUALITY STATEMENT:

10.1 In line with duties under Section 75 of the Northern Ireland Act 1998; Targeting Social Need Initiative; Disability Discrimination Act 1995 and the Human Rights Act 1998, an initial screening exercise, to ascertain if this policy should be subject to a full impact assessment, has been carried out.

10.2 The outcome of the equality screening for this procedure undertaken on 1st June 2022 is:

Major impact ☐
Minor impact ☐
No impact. ✓

11.0 SIGNATORIES:

Sheridan Easter

Sheridan Easter **Date: 23rd June 2022**
Lead Author

Maxine Paterson

Maxine Paterson **Date: 23rd June 2022**
Lead Director

APPENDIX 1 – CONFIRMATION OF TRAINING AND TERMS OF USE FOR BWV:

BWV 1 - Confirmation of training in use of Body Worn Video devices and declaration statement of responsibilities.	
Full Name: (PRINT)	
Date:	
Role/Position:	
Directorate:	
Division:	

1) I have received appropriate training in the use of Body Worn Video equipment, and fully understand the operation, activation and maintenance of the Body Worn Video Device. I understand the reporting mechanism, if required for lost or damaged devices.

2) I have read the Body Worn Video Policy and Procedure in full. I fully understand my legal obligations of using the Body Worn Video device under the legislation contained within this policy and procedure, and fully agree to adhere at all times, to same.

3) I understand and accept that it is my responsibility to ensure the body worn video device, when in my possession, is used appropriately and proportionate to the situation. Any deviation from the strict use as detailed within the policy and procedure may result in disciplinary action.

4) I have no further questions or queries in regards to the operational use of Body Worn Video devices.

By way of signature below, I agree and acknowledge to the terms and conditions as per the "*Northern Ireland Ambulance Service Health and Social Care Trust"* Policy and procedure on Body Worn Video use.

Print Name:		**Sign Name:**	
Date:		**Time:**	