HSC Data Protection Impact Assessment (DPIA)

The Data Protection Impact Assessment (DPIA) outlines what personal data will be processed, the uses of the information and any risks associated with the processing and steps taken to mitigate against the risks.

Project/System name	
Piloting the use of Body Worn Camera (BWC) devices by Nursing staff in an Emergency Medicine Department	
Divisional Project Lead – completing the DPIA (name and contact details)	
Divisional Lead/Governance: Edward M. Smyth Divisional Governance Lead Medicine and Emergency Medicine	Antrim Area Hospital Bush Road BT41 2RL EdwardM.Smyth@northerntrust.hscni.net
Department/Location	
Department: • Emergency Department, Antrim Area Hospital Service/Operational Lead: Gerry Gallagher ACSM ED & AIAO for ED Medicine and Emergency Medicine Antrim Area Hospital	**Locations for use**: • Ambulance Triage; • Ambulatory Emergency Care (AEC) • Majors; • Observation unit.
Directorate/Division	
Division Associated with Pilot: Emergency Department is aligned with the Medicine & Emergency Medicine Division. **Project Owner:** Executive Director of Nursing, Midwifery and AHPs and Divisional Director Paediatrics, Women's Services and Corporate Support. **Project Lead:** Assistant Director of Infection Prevention and Control (Nursing) **Project Group:** Chaired by Corporate Project Lead (Assistant Director, Infection Prevention and Control) and consists of representation from the pilot division, nursing and corporate support services (CG, IG, ICT, ICT Security & Governance, Equality Unit, HR, Estates).	
Date DPIA commenced	
Mid-April 2024	
Version number	
0.1 – first draft (for DPO consideration, prior to presenting to project group)	

STEP 1. DESCRIBE THE PROCESS

Briefly describe below the purpose of the data processing and what the project aims and objectives are?

Please **do not** embed documents or hyperlinks. Instead, attach relevant documents as appendices and clearly indicate which section of the appendices provides the necessary info in relation to each question below.

- **what information will be collected,**
- **how it will be collected,**
- **how it will be used / processed**
- **where it will be stored**
- **who will have access to it (including any 3rd parties)**
- **the arrangements for and when it will be deleted**

Introduction

The Northern Health and Social Care Trust ("the Trust") has two Emergency Departments (EDs), situated across two sites – Antrim Area Hospital and Causeway Area Hospital. It also has a Minor Injuries Unit on the Mid-Ulster Hospital site. The Emergency Department (ED) in Antrim Area Hospital has the highest activity of the sites. During the period Apr-23 – Mar-24, there were 101,692 attendances in Antrim, which was 64% of the total ED attendances within the Trust. This number does not include those individuals who accompanied individuals attending for treatment. It also does not acknowledge the increasing numbers in demand of our services and the increased acuity of those who present for treatment. Despite healthcare staff working hard to provide the best possible care to patients, there has been a marked rise in acts of violence and aggression against staff over the last number of years. This is not unique to the Northern Trust and has been recognised across the region and United Kingdom. We support our NHS colleagues in condemning any incident of violence or aggression towards hospital staff, or any other emergency worker. The Trust has a duty to ensure the safety of its staff and will continue to work closely with our partners to identify further ways that can prevent such offences.

Research suggests nursing staff have higher exposure to incidents and are presented as a vulnerable cohort due to the nature of their work, which brings them into close contact with people in non-ordinary situations that can easily generate tension. It also suggests staff in the ED are more likely to experience violence than in other areas of health care. In the UK, the Royal College of Nursing (RCN, 2017) voiced concern at a reported 28% occurrence of physical violence among 6,000 nurses surveyed. Similarly, the Royal College of Emergency Medicine in 2019 expressed its concern about the rising violence against those working in the NHS and especially those working in ED. Statistics from the RCN and NHS Employment Surveys and Northern Ireland Health Trusts show continued high incidences of violence and aggression against nursing staff. In addition, the HSENI in its annual report state that assaults/violence accounted for the third highest category of incidents resulting in an "over 3 day injury" during 2022-23.

The Department of Health of Northern Ireland in December 2023 reported that over the last five consecutive years, there have been over 50,000 attacks on healthcare staff across the region. In response to rising trends, the Department of Health developed a regional Violence and Aggression framework (MOVA), underpinned by Health & Safety Legislation, which is titled "It's not part of the job" that sets out the HSC's commitment to ensuring the prevention, reduction and management of violence and aggression towards staff. This regional MOVA Framework is adopted by the Trust and recognises that staff have the right to feel safe from the threat of violence and aggression. It is recognised that the impact of violence and aggression towards staff, is far reaching for an organisation, in that it can lead to reduced performance, both individually and at team level, low morale, poor employee relationships, high levels of absence, difficulty in recruiting and retaining staff and negative publicity. When incidents do occur, it is vital that all incidents of violence and aggression are dealt with appropriately and that staff are supported in line with Trust policy.

The ED environment is highly pressured, busy and at times is unpredictable. Incidents of violence and aggression only make staff jobs more difficult. The Trust is committed to staff safety and in working to achieve a reduction in volume and severity of incidents of violence and aggression towards staff, through the provision of safe ways of working and effective training. The MOVA Task and Finish Group, which reports to the Trust Health & Safety Committee, are proposing the commissioning of this pilot as one of many interventions which are part of a toolkit to manage risk associated with violence and aggression. Other interventions adopted by the Trust include, but are not limited to, the use of communication, risk assessment, provision of de-escalation training and prevention planning, service user involvement and learning from incidents.

Baseline Data

Risk Assessments

Within the Trust, a number of risk assessments have been carried out with regards to violence and aggression across wards and services. These have been led by the Health & Safety Manager in consultation with the MOVA Group. The assessments indicated more is needed to be done to protect Trust staff. As part of its response, the Trust have been rolling out "CPI training" since January 2023 to provide staff with skills to help them recognise distress/challenging/aggressive behaviour and to help them de-escalate or respond to that behaviour. The level of training which staff ultimately receive is informed by the outcome of their aligned ward risk assessment

Volume and Nature of incidents

While Trust staff are expected to report any incidents of violence and aggression using the Trust incident reporting system ("DATIX"), as part of normal business, there is often occasions due to the busyness and demands of the clinical setting that may limit staff capacity and ability to report incidents in a timely manner or at all. Accordingly, defining the exact nature and prevalence of violence has always been problematic. As early as 2002, research (Krug et al.) reported the difficulty in getting an accurate measure of the scale of the phenomenon due to incident reporting not always being completed, even in health services that supported reporting. Recent studies show, little has changed and there is still a perception of under-reporting by nurses (Ayasreh & Hayajneh, 2021). The current evidence, in research and anecdotally, of direct reduction in the volume of incidents following use of intervention is contradictory. It is the sub-groups understanding that the relationship with incident reporting is not so linear and the Trust acknowledge there is a possibility incident reporting could increase following the introduction of BWC devices for the pilot as protocol will require BWC Operators to report incidents following activation of devices/recordings. This however would be expected to balance out and be more reflective of actual incident levels (with acknowledgement of aforementioned under-reporting and the regional and national increasing trend of V&A type incidents (possibly due to wider social factors)). Balancing factors for this would be an expectation that the
Average weighted severity should reduce; increased staff psychological safety, job satisfaction and time spent dealing with incidents/complaints or attending court to provide evidence.

Below is an outline of reported incidents, which signals growing numbers and identifies the types of individuals affected and the nature of the types of incidents. The Trust recognises the actual number of incidents may not decrease when BWC devices are deployed and in fact the use of this technology may inflate reporting of incidents that may not previously have been reported by busy staff or staff who have a higher threshold perception of Violence and Aggression and/or see it as part of working within the setting, but regards of volume it is hoped the severity of incidents lessen.

Corporate NHSCT V&A (Annual picture)

2022	2023	2024
1968	2505	2570
3 Year average		2348

Antrim ED by sub-category (incidents where staff were victim to violence only)

	Physical	Verbal	Other	Total	Equates to	PSNI attend?
2022	22	19	2	43	*Approx. 15% of AAH incidents*	10
2203	25	30	1	56		19
2024	22	13	4	39		12

Source: Trust Health & Safety Department supported by the Corporate Datix Team

Examples of hospital violence and aggression incidents:

Physical & Verbal aggression	• Patient clenching their fists when approached by staff. • Patient verbally and physically aggressive towards clinical and security staff. Punched window several times and the cardiac monitor numerous times until screen smashed. Also broke oxygen point. • Patient bit ED Registrar on finger and broke the skin. • Patient physically and verbally abusive to staff. Nursing staff and carer punched, grabbed and spat at. • Patient become very aggressive and hit health care assistant in chest and kicked and punched their abdomen. • Patient verbally abusive to nurse and hit nurse on face with ECG lines leaving mark along their jaw line and breaking the ECG clips. • Patient with mental health issues ran out of cubicle and into another area of the ward. When doctor approached patient they pointed a sharp object at them, which appeared to be a knife. • Patient with alcohol and drugs on board became very aggressive and abusive in waiting area making patients and staff feel vulnerable. • Patient aggressive and threatening patient in next bed. Also staff who intervened
Sexual/ Inappropriate behaviour	• Patient slapping and grabbing other patients and staff on the bottom and trying to kiss patients and staff. • Patient exposed himself in front of staff, visitors and patients whilst urinating on the floor.

Related News Articles

Dec-23: Health care attacks: Pregnant doctor among those assaulted

Apr-24: Warning sounded over NI hospital staff safety: 'It is pure luck somebody hasn't been killed'

What is being proposed?

The rollout of x12 Body Worn Camera (BWC) devices in the ED at Antrim Area hospital as part of a three month pilot, starting Mid-2025. BWC devices will be utilised by uniformed nursing staff only in x4 areas within the ED, notably the Ambulance Triage, Observation Unit (Obs), Ambulatory Emergency Care (AEC) and Majors. However, depending on the success of the pilot, consideration may be given at a later stage to expanding use of devices in other locations and sites.

Uniqueness

While this pilot will be the first time BWC devices have been deployed by the NHSCT and in an ED setting regionally within Northern Ireland, use of the technology within healthcare settings is more prevalent when looking more broadly across the UK and examples can be seen in many NHS organisations, including many ED settings (e.g. Bristol, Barts, Gloucestershire, RDH, UHCW and NUH etc.).

Why the ED?

The Sub-Group assigned to develop and coordinate this pilot recognise that the context which surrounds ED incidents is unique in many ways when compared with acute and general ward settings. In the latter, the number of patients present is relatively fixed and wards know who is present (inpatients); there are less unknown individuals accompanying patients and/or sporadically coming/going (with visiting rules in place); there is access to full hospital record/notes (under current manual system) and given consideration to

prior/existing illnesses, characteristics and risks (including alcohol and drug dependencies) will form part of care planning; staff may recognise patterns of patient behaviour over the duration of stay making individuals more predictable (more likelihood of repeat incidents of similar nature involving same individuals). Unlike ED, where there the environment is less controlled and more chaotic with higher volumes and generally more acutely unwell patients. In the ED there are many individuals present who are not patients and may not be known to patient and/or staff and many individuals coming/going sporadically, leaving the environment and the behavioural characteristics of those who populate it less predictable, which could translate into incidents of a more serious nature.

Why are we doing it?
Our legitimate interests for pursuing this pilot are set out under Step 4 (below).

Any form of violence or aggression directed towards others is not acceptable nor should it be tolerated. Organisations must be vigilant in ensuring that support and reporting violence are more accessible and streamlined. While all forms of violence in the workplace are a challenge, physical violence, and its potential for severe harm, is a cause for concern within the ED in terms of physical, psychological and social outcomes.

The Trust recognise that this ongoing issue has serious, long-term impacts on the Trust's ability and capacity to deliver its services. Such incidents can have a negative and detrimental impact on both staff and/or patients and visitors and have potential to inflict personal trauma. Staff who sustain assaults may need to take off work and seek medical and/or psychological support, all of which having a knock-on effect on ward capacity and are a financial burden for the Trust. Also, in such busy and turbulent environments like ED, there is a danger that staff frequently exposed to aggression and negative behaviours may start to normalise the instances as being a by-product of working within the ED setting, particularly if they perceive an inability to change the "status-quo". Such acceptance could spill over to negatively impact the workforce culture, job satisfaction, staff absences and the Trust's ability to recruit permanent staff into the ED.

Research suggests that BWC devices can be an effective tool in response to violence and aggression and have been shown to be effective in healthcare environments and that use of the technology is generally accepted provided controls are put in place. Accordingly, this small-scale pilot initiative, applying the use of BWC technology as part of a preventative strategy to reduce frequency and/or severity of untoward events which could compromise safety of individuals, is not expected to cause any new impositions to patients, staff and/or other third parties visiting Trust premises. It is anticipated this pilot will from good learning and best practice should the Trust wish to consider further roll out of BWC devices across other areas within the Trust.

While staff in the ED are trained or being trained in managing incidents where individuals may become violent or aggressive, there are occasions when experience and expertise are not enough to defuse a situation. In such cases, having a BWC device would provide additional support and an added layer of safety for them and those in proximity. More, the use of BWC has now been widely adopted in other geographical areas of Northern Ireland in Healthcare. Both BWC devices and CCTV share similarities in terms of their assumed causal mechanisms. Both are rooted in deterrence theory with their presence expected to convince potential aggressors to desist from engaging in delinquent and challenging aggressive behaviour. In Northern Ireland a growing body of evidence for use in Healthcare has been further enhanced by the recent introduction of BWC by the Northern Ireland Ambulance Service (NIAS) and Southern Health and Social Care Trust (SHSCT). For these reasons NHSCT, Senior Management Team (SMT) gave approval on 9th January 2024 for the BWC Project Team to move to preparation for Public Consultation ahead of a pilot to support staff in dealing with increasing numbers of incidents of violence and aggression in ED.

Anticipated Benefits

- Support staff and generate awareness to support;
- Increase staff psychological safety at work and help bolster staff morale and satisfaction by making real and perceived improvements to healthcare environments;
- Directly or indirectly reduce incidence and severity of violence and aggression towards staff;
- Help deliver improved patient care through calmer environments;
- Improve the education of staff on management and prevention of violence and aggression;
- Deliver cost savings, reducing the actual and associated costs of violence and aggression incurred

Beyond scope

It is important to recognise that the wider issue of violence and aggression in society does not start or end in a healthcare setting. A comprehensive approach to this subject would consider the numerous social and environmental catalysts for violence and aggression outside of the ED. Within the ED environment, violence and aggression may occur as a result of these wider social factors. For example, acts of violence and aggression occurring as a result of – or that are directly related to – drug and alcohol consumption or mental health. This pilot does not attempt to address all the reasons why violent or aggressive incidents take place or seek to present a total solution to the problem.

How will this be co-ordinated?

In preparation for a potential pilot, a Trust sub-Group was established late November 2023 to discuss the concept. Later, following SMT approval in January this group was tasked with giving consideration as to how to operationalise and to scope the necessary legislative and policy requirements (i.e. Privacy, Data Protection Legislation, Equality, Human Rights etc.) and available solutions from Suppliers and associated costs. The sub-group responded by conducting research and pre-consultation engagement with a number of key stakeholders across Northern Ireland and England. This DPIA is a product of this sub-group as is the supporting documents that accompany it and form part of the Trusts preparation to go out to consultation which shall inform any further consideration of the proposal and decision as to whether the pilot should proceed.

<u>As set out below, this small-scale pilot has x4 main phases. *Prior to Public consultation, the focus is Phase one.</u>

Phase 1: Scoping and Planning

- Identify product offerings;
- Quotations;
- Stakeholder mapping and engagement plan;
- Pre-consultation engagement with key internal and external stakeholders via mixture of methods (F2F meetings, MS Teams, pre-intervention baseline survey);
- Drafting suite of key documents to support any consultation and/or pilot and Trust management consideration/decision;
- Seek Trust approval to proceed to Public Consultation

Phase 2: Evaluation and Refinement

- Run Public Consultation 14 weeks;
- Evaluate outcome of Consultation;
- Adjustments to suite of key documents and any further pertinent actions informed by consultation;
- Seek Trust approval to continue to Pilot;

Phase 3: Implementation of Intervention

- Pilot (subject to approval) – 12 weeks;
- Maintain project documentation and local highlight/KPI reporting to MOVA Group and Divisional S&Q.

Phase 4: Evaluation and Results

- Post-pilot evaluation survey
- Evaluation of Pilot report to inform consideration of longer-term adoption
- Close loop/Share Learning

Timeline for Public Consultation

This DPIA is drafted with a view that approval of this draft along with supporting documents will be sought at the end of January 2025 for the Public Consultation to commence February 2025. The Trust are mindful that we are undertaking this consultation during the summer months. We are committed to hearing stakeholder views and to facilitate this we hold the consultation period for 14 weeks. The consultation will include a number of engagement events (online via MS Teams and in-person), as well as X-Social platform engagement. Provided Trust Board support the continuance of the pilot following consultation, training and SOPs will be provided to the designated staff selected to be involved in the pilot.

NB: this DPIA will be revisited following the Public Consultation and any necessary revisions made prior to seeking further approval from SMT to continue. Should approval be granted, at that point it would be Task and Finish Groups intention to deploy BWC devices at the earliest opportunity.

Intervention

The pilot will be fully supported by Calla (Supplier) and this will include:

- Calla Body Cameras,
- Docking Stations,
- Camera + Software Support,
- Camera licensing,
- Dedicated Account Manager,
- Product & software training session,
- Support in setting up the Governance and IT aspects of the project.

Body-worn camera devices are a wearable audio and video recording system used to record events in which the wearer is involved. In selecting a BWC device for the pilot, the project group conducted a scoping exercise to ascertain available BWC products and the prices ranges. It became apparent that currently a large proportion of BWC products are relatively bulky and seem to be marketed more towards security roles, which the project group felt limited product options as this is not the target staff group for the pilot. The BWC device ultimately selected was designed with healthcare in mind and is small, non-intrusive and has been piloted successfully in another Trust within Northern Ireland (SHSCT) and in many NHS organisations in England. The BWC selected for the pilot is the Reveal Media Ltd Calla BWC device. The Calla BWC is small in size (is 57mm in height, 43mm in width, has a depth of 17mm) and light (weighs 90g). Devices can be mounted via magnet mounts, crocodile clips, lanyards and klick fast stud options. The devices are robust and have IP54 protection, a 1.51 LCD display and are powered by a Lithium Polymer (750mAh) battery providing a life of up to 2hrs on 480p quality recording and 1.5hrs on 720p quality recording in MP4 and ACC formats. Device charge time from flat is 2hrs by microUSB. On-screen display features include Icon Indicators, Live View, Date/Time, Memory and Battery. Notifications are communicated via Audio, LED and LCD. Devices have a storage capacity of 16gb and are AES 256 encrypted and have a field of view recording is 90 degrees horizontal and 50 degrees vertically.

Digital Evidence Management Software (DEMS 360) the accompanying software is built within the scope of ISO27001, with PEN testing to ensure data security. It is a central solutions management software that supports all BWC video, images and audio files. It is simple to maintain configuration, settings and user permissions and can be deployed On-Prem or within a Reveal managed Microsoft Azure Cloud environment. The solution is scalable with unlimited users and storage to grow a project without impacting performance.

Access to data and functionality is controlled via user authentication and permissions with a complete audit log of system activity. All data will be protected and set to be retained in line with Trust policies.

What Data will be Collected/How will it be Used?

BWC devices are unique in terms of their mobility and flexibility, unlike CCTV cameras, which tend to be static and mounted on walls or ceilings. The agreed number of BWC devices assigned to staff for the pilot will be used to collect data. Initially, the pilot will only involve nursing staff and staff selected for use of devices will be based on their area of work within the ED. Staff will be selected by the Sister and Assistance Clinical Service Manager (ACSM). Staff participation nonetheless will not be mandated during the pilot, but any refusal to participate will be noted only for pilot evaluation purposes.

The BWC devices, when activated, will collect both direct and indirect primary and secondary audio and video information relating to the environment surrounding the staff member wearing the device, which will include staff, patients and possibly third parties. Examples of primary information will comprise of first accounts from individuals, person identification, direct conversations, decisions and actions of both the staff wearing the BWC and those in within range of the camera; one's physical and mental state and demeanour and location. Staff with an attached BWC may also unintentionally capture secondary information such as access codes to ward buildings and/or devices, radio communications, information relating to staff and other emergency personnel such as visual and verbal identification, staff in a distressed state, name badges/IDs, and potential similar information relating to third parties who happen to be in the proximity while the device is in use. However, training will focus on how to reduce collateral intrusion.

BWC devices will be used in accordance with a set activation criteria and deactivated when staff perceive the risk to have decreased. BWC devices will be activated when there is either a violence or aggression type incident taking place or when a situation is unfolding that staff perceive could likely escalate into a more serious situation or incident which could put Trust staff, property and assets at risk. During the pilot, activation will be triggered by staff only. While there is potential that individuals in the ED may ask staff wearing BWC devices to activate their camera, activation will only occur should the staff member conduct a dynamic risk assessment and conclude circumstances met the set activation criteria. It is acknowledged staff perception of perceived risk may be influenced by their own experience and exposure to violence and aggression within the ED setting.

Activation Criteria:

Any incident, in which a person is abused, threatened or assaulted in circumstances arising out of the course of their employment or where Trust property or assets are put at risk or damaged.

This includes:

- **Threatening behaviour: including bullying, intimidation, psychological abuse, harassment, inappropriate use of social media and/or telecommunication and threats with weapons.**
- **Verbal abuse: the use of inappropriate words or behaviour causing distress including shouting, swearing or insults with racial or sexual intent and intimidation.**
- **Physical violence: the intentional application of force to another person without lawful justification, resulting in physical injury or personal emotional discomfort. It also includes slapping, punching, nipping, biting, kicking, spitting, butting, head butting, stamping or sexualised abuse. It may also include more extreme forms of violence using weapons that are not just restricted to sharp implements, chemicals and firearms.**

In addition to deliberate acts of violence and aggression that are sometimes displayed by service users (or their family and friends), illnesses and mental capacity may also lead to unintended or unintentional incidents of violence and aggression which are outside of their control, but which lead to the harming of staff. Activation will be motivate-blind, but circumstances surrounding activation will be given due consideration when Trust management are reviewing and labelling footage and will inform the response taken.

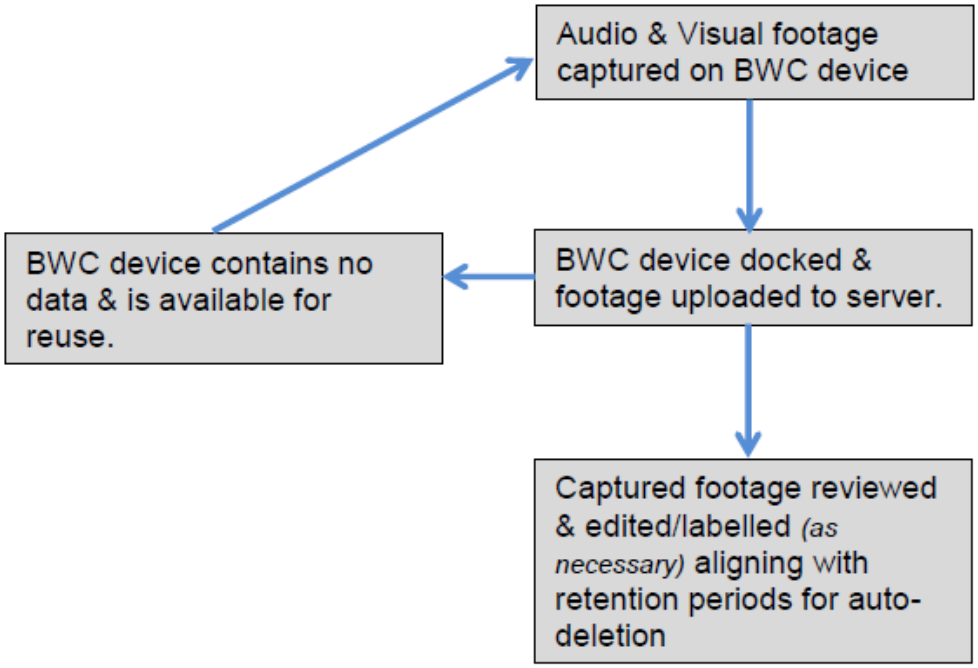
Source: Adopted from the MOVA Framework

Both activation and deactivation is done manually and recording of audio or visual data will not occur, unless a device is activated. This will be informed by Trust policy on use of the BWC devices. Protocol will stipulate that any staff, patients or members of the public in proximity at time of activation or deactivation of a BWC will be made aware of the intention to activate or deactivate the device by the staff member making a verbal announcement before manually triggering the recording or cease recording function. When recording mode is activated a red-light will appear and the footage will be displayed on the front-facing screen. Use of the devices within the ED setting will also be publicised through use of posters/signage at entrances/exits and the ED TV/Rolling screen within the waiting area and a Privacy notice will also be accessible to those visiting the ED.

Process

- Staff need to be trained on use and management of BWC devices and have undertaken the necessary complementary mandatory training prior to involvement in pilot. *(Please see section 3.3 of policy).*
- Allocated members of ED nursing staff within the intervention areas will attach BWC devices to their uniforms and wear devices for the duration of their shift.
- Devices will be signed out from the Sisters Office in the ED. (*Please see Appendix 3 BWC Device Allocation (Sign Out/In) Log Sheet*).
- Devices must be signed back into the Sisters Office in the ED. (*Please see Appendix 3 BWC Device Allocation (Sign Out/In) Log Sheet*).
- Device will not be recording until activated. Activation of the BWC must be incident specific and users should not record day to day activities. (*See Activation Criteria and Point to Start Recording section of policy*).
- Decisions to record or not to record any incident remains with the staff member wearing the device. (*See sections of policy on Cessation of Recording and Partial Recording*).
- On activation of the device, the staff member should make a verbal announcement to indicate recording is to commence.(S*ee Activation/Recording section of policy*).
- Any recording of a patient/service user should be noted in patient clinical notes, registered in the Device Event Recording Log and linked to any Datix submitted. Datix reports should have the check-box completed indicating BWC footage has been recorded and should include the BWC Footage ID and Name of Operator/IR. (*Please see Appendix 4 BWC Device Event Recording Log Sheet in policy*)
- On deactivation of the device the staff member should make a further verbal announcement to indicate recording is to cessing. (*See Cessation of recording section of policy*).
- Following any recording of an incident and/or at the end of a shift, devices should be docked again in the Sisters Office in the ED. This process allows for automatic upload of data to the server and charging –Uploader software is used for this on client PC and highlights status of transfer for users. Devices should be regularly inspected by BWC Operators/IRs following each incident and shift and docking should be registered on the log sheet. (*See Appendix 3 BWC Device Allocation (Sign Out/In) Log Sheet in policy*).

Data Flow



Data Storage/Retention/Access

Data captured will be held strictly in accordance with the UK-General Data Protection Regulation (UK-GDPR) 2018 and the Data Protection Act (DPA) 2018, and consideration will also be given to the Trust IG and ICT policy frameworks and other related policy (i.e. Forensic Readiness, Trust Retention Schedule (GMGR)).

Data management will include the following guiding principles:

- All personal data will be obtained and processed fairly and lawfully;
- Personal data processed will be adequate, relevant and not excessive in relation to the purpose for which it is processed;
- Personal data will be processed only for the purposes specified;
- Personal data will only be disclosed to Trust Officers and other third parties (such as the PSNI) as authorised by the Trust Information Controller in accordance with existing Trust Procedures and/or extant legislation.
- Personal data will be held for no longer than is necessary;
- Personal data will be processed in a secure manner with procedures put in place to ensure data is correctly and safely transferred from BWC devices onto a secure Trust server;
- Individuals will be allowed access to information held about them, where appropriate and where requests are made and assessed as appropriate in that no harm may come to an individual should they achieve access;
- Procedures put in place to prevent unauthorised and/or accidental access to, alteration, disclosure, or loss and destruction of, information;
- Staff using BWC devices shall undergo training before they operate devices and training package to include: reference to legal implications; Data Protection Legislation; Human Rights Act.

Default settings for BWC devices will mean that devices will only store data if the record button is activated by a staff member. Data held on the BWC device is encrypted to AES256 standard and temporarily stored on internal memory and via use of an RFID card within the device and remain encrypted at point of transfer using either a docking station or via USB (backup transfer option should docking stations malfunction). Docking will occur routinely

either after each shift or immediately after an incident. The location of docking stations will be in secure and accessible location(s) within the ED, located near the Sister's Office. Once the BWC device has been docked, the data transfer process will be automated, encrypted and data transferred to a dedicated secure Trust server which is a government approved Microsoft Azure cloud platform for 28 days unless the file is labelled as having evidential value for the investigation of an incident. Once data is transferred from the BWC device to the secure hosted cloud server, all data previously held on the device will be erased.

All data files from BWC devices will have a unique reference to ensure the data can be stored within a structured filing system enabling future search and retrieval. Technical metadata will be applied to BWC devices automatically and this will include start time and date, length of recording, image resolution, frame rate, file size. Images and audio captured by BWC devices cannot be replayed on the BWC device itself by staff and requires docking for transfer to servers and access to the specified video management software to decrypt/code/playback recordings. Access to view BWC footage will be restricted to a small number of designated/authorised staff with permissions to access the designated BWC video management software (DEMS 360). Access to the software requires a unique login ID and software usage includes an audit trail. As part of this DPIA, the project team will ensure the software is compliant with HSC security and information governance requirements

Should information be requested by an individual on the use of BWC devices or BWC data requested by individuals captured on footage (or a third party representing interests of an individual captured) or footage requested by the PSNI for reasons such as crime prevention and public safety following an incident to inform evidence being gathered for the PPS/Court or other proceedings, the request will be considered on its own merits/ on a case-by-case basis and handled in accordance with data protection legislation and supported through existing Trust Information Governance procedures (i.e. for handling of Freedom of Information Requests, Subject Access Requests, Police (Form81) Requests. BWC software has capability for creating ISO copies of recording for burning onto disc format and this can be utilised for requests (**ISO referring to file type - identical storage image of optical media*). This is similar to how requests for CCTV footage are dealt with by the Trust, but with a distinction that there are additional privacy considerations when evaluating the release of BWC footage due to there being both audio and video data. Additionally, any organisation with statutory powers (e.g. Police Ombudsman, Health and Safety Executive etc.) may also be able to access a record to support their own investigations. Again, such requests will be considered by the Trust on a case-by-case basis. All public sector parties receiving data will be registered with the Information Commissioner's Office and have a duty to comply with legislation and have organisational Information Governance frameworks, including policies, procedures and training protocols for the management of data held. While a data subject is entitled to their personal data they are not entitled to personal data relating to third parties, especially if this could cause that person harm. The BWC DEMS 360 software that accompanies BWC devices has image redaction and pixilation functionality which can be adopted, as necessary, to comply with privacy and data minimisation principles.

Further detail on record management and access management can be found in the aligned Trust BWC policy and within Step 8 (below) under data minimisation.

Governance

The following principles will apply to this BWC pilot project:

- BWCs will only be used for a specified purpose, with legitimate aim and necessity to meet an identified pressing need.
- The effect on individuals and their privacy will be taken into consideration with regular reviews to ensure use of BWC remains justified.
- The NHSCT will be transparent regarding use of BWC and will have a specific privacy notice accessible online and in the ward setting, which will include a published point for contact to information and complaints.

- The NHSCT will embed clear responsibility and accountability through its governance documents for all BWC system activities, including image and information collected, held and used. This will provide clarity on operation.
- Data minimisation principle will be adopted, in that no more images and information will be stored than that which is strictly required for stated purpose and data will be deleted once purposes have been discharged in line with NI Regional Records Management protocol (GMGR).
- Access to retained data will be restricted and there will be clearly defined rules through a record management policy on who can gain access and for what purposes.
- Staff using the BWCs will be trained and will have consideration of any approved operational technical and competency standards relevant to the systems and its purpose to enable them to work to meet and maintain said standards.
- BWC data will be subject to security measures to safeguard against unauthorised access and use.
- Effective review and audit mechanism will be put in place to ensure the legal requirements and associated policies are complied with in practice and regular reports will be published and monitored by the MOVA group.
- When BWCs system is introduced, feedback from users will be actively been encouraged and acted upon. This will include the checking of understanding of how and when they activate BWC and use of data/images and any suggestions for improvement will be welcomed.

STEP 2. ASSESS THE NEED FOR A DPIA				
Screening Questions- The following are intended to help decide whether a full DPIA is necessary.				
No.	**Question**	**YES**	**NO**	**Either way please provide further details here**
1.	**Does the project involve collecting new/additional personal information about individuals?**	☐	☒	Yes. New information will be collected in the form of audio data combined with video footage when BWCs are in use. CCTV is already in operation within the hospital and grounds, but the current system in operation records video footage only. The Trust is aware that the addition of audio recording is a greater infringement on the privacy of staff, patients and members of public who are in proximity, but equally recognise the inclusion of audio improves the quality of evidence captured should data be needed in the event of an incident and/or an act of violence or aggression directed to/by staff, patients and members of public. This is because video alone can fail to adequately provide full context of an event and the addition of audio can address this and on occasions where a camera may not be capturing an event fully due to its positioning. The added context is considered an advantage for all parties concerned and can function as an independent account of what occurred.
2.	**Does the project involve gathering**	☒	☐	BWC devices are a new technology which are not currently used in the NHSCT or any other ED setting within the NI region.

	information in a new way?			Considering that these devices will be worn by clinical staff, there is the potential for more data to be obtained than by the static CCTV system and the BWCs used by Security Officers. This will be managed through training and the SOP.
3.	**Does the project establish a new way of identifying individuals?**	☒	☐	Individuals may be identifiable by combination of audio and video recordings.
4.	**Will the project use an individual's personal data already held in an existing system (manual or electronic) for a new purpose or in a new way?**	☒	☐	New technology use. No existing processing of this nature. Individuals may however already be captured on existing CCTV in proximity to the ED environment.
5.	**Will the project disclose or share personal information with organisations or people/staff who have not previously had routine access to it.**	☒	☐	In certain circumstances, (such as investigations, serious or criminal incidents) the NHSCT may need to disclose BWC footage for legal reasons. In such circumstances, the receiving organisation will be required to adhere to data protection principles. BWC footage evidence may be released to the PSNI for the reasons of crime prevention and public safety/in the event of a criminal act and in support of the investigation. The NHSCT already has protocols in place, in accordance with data protection legislation, for the sharing of information with PSNI.
6.	**Will the project involve matching or linking with personal information held by a different organisation(s) or departments or in different datasets e.g. combining, comparing or matching personal data obtained from multiple sources**	☒	☐	Matching or linking of personal data will not be routinely conducted by the NHSCT. However, should an incident occur, the footage reference number will be linked to a Datix incident report and the latter may refer to what is captured by the BWC. In addition, if BWC footage is released to PSNI they may be able to identify, for example, an attacker/perpetrator from information they already hold in their systems.
7.	**Will the project change the way personal information is managed, stored or secured (e.g. new database, new location, cloud storage)**	☒	☐	Use of BWC in the NHSCT is new technology use. There is no existing processing of this nature within the NHSCT or within ED settings across the region. As part of the introduction of BWCs, the NHSCT will consider the management, storage and security of the data processed. This will include consideration of the security of the data on BWCs worn by NHSCT staff and transfer of data with controls put in place e.g. device encryption, transfer of data to local servers and asset management. In line with the data minimisation principle, data

				will only be captured when the device is activated and retained should there be an event which meets NHSCT protocol for activation and/or retention. There will be no continuous recording by the wearing of these devices.
8.	**Is this a system or process that has not had a DPIA completed previously?**			New ☒ Update ☐

If you have answered <u>YES</u> to any of the above, <u>continue to Step 3</u> and complete the DPIA.

STEP 3. DESCRIBE THE PERSONAL DATA BEING COLLECTED		
**What Personal data is being collected? This applies to any stage of the process (tick only those that apply). ****this list is not exhaustive*		
Personal Data required	**Tick all that apply**	**Provide details of who the personal data relates to:** i.e. Service User/staff/relative/Other (please detail)
Name	☐	Unlikely but there is a potential should the individual or another nearby volunteer the information during a recording.
Address & Full post code	☐	
Date of Birth	☐	
Work email address	☐	
Personal email & Mobile	☐	
National Insurance number	☐	
Health and Care number	☐	
Hospital No./System ID	☐	Unlikely but there is a potential should a staff member involved raise this in conversation.
Personal Images	☒	Potentially footage could show some health information/interferences – i.e. individuals being on drips, wounds visible, using breathing apparatus etc. Identifiable video images of patients/service users, members of the public and staff may be captured by BWC devices and stored on secure servers.
Other*	☒	Audio associated with staff/patients/service users and members of the public may be captured by BWC devices and stored on secure servers.
Please provide justification for the personal data being processed e.g. Do you need full postcode or would partial postcode be sufficient? Do you need full Date of Birth or would age be sufficient?		
The use of BWC devices may raise some concerns around processing given that recording will take place in an area that patients would not normally expect and with there being potential vulnerability of the data subjects. However, the approach to Public Consultation and the drafting of the governing documents is aimed at minimising any potential risk or intrusion, with a view to offer assurance to the Public regarding the legitimate aims of the Trust. BWC devices will collect images in the form of video and this is combined with audio and therefore will have capability of processing background secondary and third-party information. It is therefore inevitable that BWC data could capture the movements and actions of other persons, not involved in an incident, when this equipment is being used (known as collateral intrusion).		

The combination of audio and video and the mobile nature of the technology will improve the quality of data collected in the event of an incident and recording will only be activated should the defined activation protocol be met. The Trust will limit the collection of personal data associated with this pilot to that which is strictly necessary to achieve the aims and data will be managed in accordance with Trust and Regional Records Management protocol.

In so far as is practicable, and in an attempt to minimise collateral intrusion on those not directly involved, staff using BWC devices will be trained to restrict recording to areas and persons necessary in order to obtain evidence relating to an adverse event. Staff will make a decision on whether or not to activate a BWC device to record mode on a case-by-case basis. No covert recording will take place and those in the proximity will be notified before devices are activated, promoting transparency. This will be referenced within Trust policy and the SOP.

Should data be requested for release for whatever purpose, the rights of all parties captured will be considered by the Trust and any third parties captured in the footage who are unrelated to the incident/event will have their identified protected and anonymised through masking of audio and the blurring of images via technology embedded within the supporting Digital Evidence Management Software (DEMS-360).

Special Category data (sensitive personal data)	**Tick all that apply**	**Provide details of who the Special Category data relates to:** i.e. Service User/staff/relative/Other (please detail)
Health and Social Care Data	☐	
Racial or Ethnic Origin	☒	
Biometric data (e.g. finger print, eye, face)	☐	
Genetic data	☐	
Data concerning a person's sex life/sexual orientation	☒	
Religious beliefs	☒	
Other: Political opinions ☐ Philosophical Beliefs ☐ Trade Union Membership ☐ Criminal convictions ☐		

Other data collection methods: If your processing includes monitoring/surveillance, body worn cameras, Virtual Number Plate Recognition (VNPR), CCTV, GPS, Fitness trackers, recording phone calls/voice information please provide more detail below:

As per above section, some personal information may be collected via audio and video which may not usually be expected during the standard care-giving processes. This will be depending on what the 'subject individual' may say during a recorded discussion. The devices have a redaction software capability which will be able to obscure anything that is not relevant to the incident or subject person(s)/assist with management of any potential intrusion to privacy.

STEP 4. LAWFUL BASIS FOR PROCESSING

What is your UK GDPR Lawful Basis for processing/sharing personal data? See Appendix 2 for further information or seek IG advice.

Article	**Lawful basis**	**Tick**
6 1 (a)	Consent	☐
6 1 (b)	Contract	☐
6 1 (c)	Legal obligation (Please detail which legislation* this will come under)	☐
6 1 (d)	Vital Interests	☐

6 1 (e)	Public Task (please detail sections of the legislation which support Public task legal basis below)	☐
6 1 (f)	**Legitimate Interests** ***Also see Legitimate Interests Risk Assessment (Appendix 1)**	☒

All personal data associated with this pilot will be processed lawfully, fairly and in a transparent manner as set out in Article 6 of the UK-GDPR.

The lawful basis for processing is Article 6(1)(f) UK GDPR as processing is considered necessary for the purposes of the legitimate interests being pursued by the Trust.

A legitimate Interests Assessment has been completed and accompanies this DPIA. Legitimate interests are specified in the BWC Pilot Privacy Notice and Consultation document.

Noted legitimate interests:

- Protect and enhance the experience of patients, staff and others who access the ED unit by helping provide a safer and calmer environment;
- Enhance the security and the protection of Trust property/assets;
- Influence behaviour by acting as a deterrent to acts of violence and aggression and aid to de-escalate of situations should they arise;
- Enhance staff education and learning on Management and Prevention of Aggression;
- Record an independent account of what happened should adverse events arise and have footage captured with evidential value to any review or investigative process;
- Support relevant authorities in the apprehension and prosecution of offenders by enhancing the type and quality of discoverable evidence should criminal or civil action be brought.

The Trust will bear in mind the eight key privacy principles and obligations when considering BWC device usage. Notably –

1. **Fair and lawful processing** – the Trust will demonstrate use of BWC is both fair and legal. Necessity will be carefully considered, with acknowledgement of the potential for intrusion, due to the nature of the technology.
2. **Limited purposes & data minimisation** – BWC devices will only record the minimum amount of personal information necessary for specified purposes.
3. **Transparency** – through the use press releases, social media, Public Consultation, posters/signage the public will be made aware of the pilot and Trust considerations. Protocol for activation and deactivation of BWC devices will involve informing individuals and how data is collected and used and individual's rights will be set out in privacy notice.
4. **Information security** – All BWC recordings will be encrypted at rest and at transfer and will be stored on a secure Cloud hosted server. Risk of theft/loss of data considered through risk assessment (see relevant section).
5. **Restricted access** – the Trust will have clearly defined rules in place covering who can access recordings and for what purposes in the form of a Trust BWC Pilot policy.
6. **Sharing** – Existing protocol in place within HSCNI. The disclosure of BWC footage and data will only take place when it's necessary for specified purposes and checks will be put in place before disclosing to law enforcement or other agencies. This will be addressed in the accompanying policy.
7. **Storage limitation** – data on individuals will be retained only for the minimum amount of time required as per type of data and then deleted.
8. **Individual rights** – the Trust will respond appropriately to any privacy rights requests from individuals (such as the right of access, right to erasure or right to complain) through existing mechanisms and with the support of the Information Governance department who centrally coordinate data requests and such communications.

Trust Corporate Information Governance team has and will continue to provide expert advice in relation to compliance with the data protection legislation and the completion of this DPIA,

with consideration of the 12 guiding principles set out in the Surveillance Camera Commissioner Self-Assessment. Actions included: display of privacy notices; agreed retention periods for recorded data; confirmation of compliance for information security on both devices and cloud storage and the data processing agreement with Reveal Media Ltd/Calla.

Other Legislative Considerations

- **Health and Safety at Work (Northern Ireland) Order 1978** and the **Management of Health and Safety at Work Regulations (Northern Ireland) 2000** - Trust has a duty to ensure the safety of staff and to provide a safe and secure work environment.

- **Investigatory Powers Act 2016** – from third party/PSNI perspective of evidence and forensic readiness considerations.
- **ECHR/Human Rights Act 1998 –** Given BWC devices are a form of surveillance, the Trust have given consideration to the SCC best practice guidance, the Information Commissioner's Office (ICO) guiding principles/checklist and other sources of information (such as the British Institute of Human Rights guidance) to support the development of this document and governing documents for the pilot. Our focus was on three rights which we think are most relevant to the use of cameras and other recording equipment in health and social care (notably Articles 3, 8 & 14) ensuring our approach is lawful, for a legitimate aim and proportionate. We have also given consideration to DoL/Mental Capacity and consulted local experts. Our protocol is drafted with this in mind and our approach is a less restrictive option (bearing in mind Art8) by only switching cameras or recording equipment on when an activation criteria is met. Our privacy notice and pilot documents set out our rationale for use and legitimate aims and safeguards. The Trust recognises many service users attending the ED are interacting with the service because they are possibly unwell or going through a difficult time in their lives or have existing diagnosis. It certainly is not our intention to distress anyone or make individuals feel humiliated or frightened (bearing in mind Art3). This DPIA and supporting documentation clearly set out our legitimate aims for the introduction of BWC devices and training and operational protocol will bear this also with a view of having minimum impact on individuals. Ultimately, the Trust wants to make staff and those who frequent the ED feel safe and not frightened. The Trust's intention to protect individuals from abuses is equally aligned with the right of being free from inhuman and degrading treatment. More, our protocol allows for professional judgement and does not propose applying blanket rules or making assumptions about people (bearing in mind Art14).

If applicable what is your UK GDPR Lawful Basis for processing/sharing special category data?

N/A

STEP 5: ASSESS SECURITY OF THE INFORMATION

Will the information be shared with, hosted by or transferred to another organisation or third party? If YES, please list all the organisations who will receive or have access to the personal data being processed:

Identified Third-parties:

- Reveal Media Ltd. (BWC device and Software Supplier and Server Host) - managed by way of contract.
- PSNI/PPS provided there is a lawful basis for release.
- Statutory Organisations with investigative Powers – by law.
- Third-party Representatives – with consent of individual recorded.

Access by third-parties will be infrequent and is only expected to be required for software or hardware maintenance and support purposes and shall be governed by a contract/licence.

Any third party needing access to the server housing the BWC data will be required as part of the contract to be registered with the Information Commissioner Office and contract arrangements will contain the necessary data protection clauses and registration requirement. Also, any granted access will be greatly restricted. In terms of 3rd Party DC staff access NHSCT data, access to customer data by Microsoft operations and support personnel is denied by default. When access to data related to a support case is granted, it is only granted using a just-in-time (JIT) model using policies that are audited and vetted against our compliance and privacy policies. The access-control requirements are established by the following Azure Security Policy: No access to customer data, by default; No user or administrator accounts on customer virtual machines (VMs); Grant the least privilege that's required to complete task; audit and log access requests. Azure support personnel are assigned unique corporate Active Directory accounts by Microsoft. Azure relies on Microsoft corporate Active Directory, managed by Microsoft Information Technology (MSIT), to control access to key information systems. Multi-factor authentication is required, and access is granted only from secure consoles.

The Trust will remain the Data Controller and the Supplier will be a Data Processor only. This relationship will be defined within the terms of the contract and any associated data flow.

Third parties and subcontractors will have security accreditations - ISO 27001, Cyber Essentials & CE+

There may be occasions when the Trust have a need to share data with other third-parties who request the data and have a lawful basis to gain access to said data e.g. third parties acting on behalf of a staff/patient/visitor who has been recorded or public organisations with statutory powers such as the Police Ombudsman, HSE etc.

Each request received by the Trust will be considered on a case-by-case basis.

NB: Public/Statutory bodies receiving data for legitimate purposes will be considered Data Controllers in their own right and will have their own retention schedules to manage.

Where will the information be:	**Sent to**	**Stored**
Within the Northern Ireland HSC	☒Trust tenants	☒
Outside the HSC but within the UK	☒Cloud, Microsoft Azure datacentre based in the UK Reveal Media utilise Microsoft 365 Purview to provide data governance: https://learn.microsoft.com/en-us/purview/purview	☒

	and utilise Microsoft 365 Compliance Manager https://learn.microsoft.com/en-us/purview/compliance-manager In addition, Reveal have recently implemented Sensitivity labels	
Outside the UK but within the EU	☐	☐
Outside the EU (if outside the EU you should add this as a risk in Step 6 and detail here how will you safeguard any international transfers)	☐ No international transfers.	☐
How will you secure the information in Transit? Tick which apply		
Encrypted Email	☐	
Shared internally over secure network	☐	
Secure file transfer	☒ SARs/Third Party Requests may be shared via platform such as Egress or the DoJ file sharing alternative (CJSM). ICT security measures are in place to maintain separation of the control system and data storage to reduce risk of unauthorized access and prevent unauthorised data interception or infiltration are: Multi-factor Authentication (MFA) Account Lockout Policies Monitoring and Anomaly Detection solutions Strong Password Policies User Education about the risks of credential stuffing attacks and the importance of unique passwords (frequent training)	
Secure Cloud Server /Amazon AWS or Microsoft Azure	☒ AES 256 Cloud Hosted Solution by Supplier, Reveal Media Ltd. Azure data centres: Resilience and availability of that data is dependent on the responses given by the authority to the document 'Reveal Cloud Data Resilience and Availability' Reveal follow the instructions of the authority as the data controller in that regard. GXO: Look after repairs of the cameras in our contract. GXO ensures that they are bound by the requirements of confidentiality, integrity, and availability of the data of the authority.	
Registered post via post safe envelopes / secure post service	☐	
STEP 6: ICT INPUT		
Have you sought approval from your IT/ICT/Digital Services Department? If **YES** continue to answer the remaining questions in this section	**YES** ☒	NO ☐
Experts from both ICT Security and ICT/Estates Representation formed part of the Task and Finish Group membership for this pilot. Protection of data on BWC devices, in transit and on servers will be of priority. This will include protocols on accessing risk factors associated to storage following receipt of the ICT Security & Technical Questionnaire by ICT security. Infrastructure - The AES256-BIT Encrypted videos are uploaded to the DEMS 360 Cloud (within Microsoft Azure UK) via USB to a bitlocker encrypted Windows Machine running the DEMS 360 Uploader service to automatically transfer files via a the securely encrypted HTTPS (TLS 1.3) protocol. DEMS 360 SaaS (Microsoft Azure UK) Reveal Media secures data using AES-256 encryption for body camera recordings and Azure SQL Database Transparent Data Encryption (TDE) for data at rest. Data in transit is protected with TLS 1.3 protocols. Any data transferring between data centres is encrypted with MACsec. WAF is used with authentication via User based login.		

Data Encrypted at rest: Cameras video files are encrypted with AES-256BIT encryption and have trusted mode (a unique key to each DEMS 360 system which renders the camera unknown to any other device it is connected to). Further detail on management of ICT and Data risks detailed in section 11 Risk Assessment.		
Has a 3rd party technical questionnaire/Cyber Security questionnaire been completed and approved by IT/ICT/Digital Services Department?	**YES** ☒	NO ☐
If the cloud storage platform is not Amazon AWS or Microsoft Azure, please answer the following questions: Has the solution been PEN tested? Does the solution have Anti-Virus software? Does the solution have Anti-Ransomware? Is multi factor authentication available?	Not applicable – MS Azure Regardless, Pen test complete/report provided. DEMS 360 V7.0 PEN Test Summary 05122(	

STEP 7. CONSULTATION PROCESS

You should consider the impact of the new process or system will have on all your stakeholders. If you have not consulted with affected staff or service users please explain your reason for this below:

Who have you consulted with?	Service Users☒ IG Department ☒ IT Department ☒ Legal☐ Internal/external Partners (please list) ☒ Statutory agencies (please list) ☒ Other (please list) ☒

Introduction

Key stakeholders and groups were identified and prioritised following a stakeholder analysis and engagement exercise undertaken by the sub-group coordinating the pilot.

Approach to Engagement

- **Pre-Consultation Engagement:** Sub-Group members identified a number of key internal and external stakeholders to either consult, network with or correspond with to help shape our Trust planning phase and drafting of key governing documents.
- **Full Consultation (14 weeks):** Provided SMT and Trust Board approve the draft documents and proposal to go out for consultation, communications regarding the Public Consultation will make use of the Trust Consultee Database of approximately 1500 stakeholder groups, including but not limited to: affected Staff; All Trust staff; Engagement Advisory Board; Human Rights Commission; Information Commissioner's Office (ICO); Involvement Network; Local Councils; Local GPs; Local MLAs/Councils; Local Population; NIAS; NIPSO; Other Trusts; Patient Client Council (PCC); Professional Organisations; PSNI; Regionals and local voluntary/community sector; Relevant stat bodies; RQIA; Service Users & Carers; Trade Unions (RCN, UNION & BMA); Media

Stakeholders:

Internal Partners	External Partners
• Communications Team • Consultants in ED/Operational Senior Management • ED staff, particularly nursing in pilot areas • Health & Safety Committee/MOVA • Human Resource Management, Employee Relations & Organisational Development • ICT • ICT Security & Governance • Information Governance/Records • Learning Disability Division • Mental Health Liaison • Paediatric Service • Patient Flow • Professional Forum/Leads - Allied Health • Professional Forum/Leads - Social Work & MCA SW Lead • Senior MEM Team & Governance • Trust Board/Exec Team/SMT/ADs	• Calla (Supplier of device); • Chief Nursing Officer (CNO) • Directorate of Legal Services • Engagement Advisory Board • Information Commissioner's Office (ICO) • Minister, DHSSPSNI, SPPG • NIPSO • Other NHS organisations/Trusts (that have piloted the use of BWC) • PSNI (Antrim District) • Security staff and G4S • Trade Union side

The process can be summarised as follows:

- Data Protection Impact Assessment (DPIA), Legitimate Interests Assessment (LIA), Equality Impact Assessment (inclusive of a Human Rights screening and rural needs assessment in one document) (EQIA) and along with a proposal documentation on the what, how, why, when for Public Consultation that will include infographics and Frequently Asked Questions.
- Easy-read versions of the Consultation proposal document will be made available (& other language translations can be provided on request).
- 14 weeks of Public Consultation commencing 23 January 2025. – This will be publicised on Trust website (dedicated area), SharePoint, social media (internal & external). Consideration will be given to print media, local news outlets, local radio and libraries (Communication Strategy) and use of direct mail to relevant persons on HSC consultee list / Stakeholders Forum list.
- Potential to directly contact specific groups and organisations identified as having significant interest and influence (e.g. Human Rights Commissioner, Information Commissioners Office).
- During the consultation we will hold an in-person event in the Antrim Area and online listening events (dates to be confirmed with speakers/facilitator) – a flexible approach will be taken to accepting additional feedback through the use of an online or hardcopy survey, in other written forms or by way of phone to the equality unit. (Meetings can be supported by video sign language interpreters through regional contract).
- Equality & PPI Team will maintain consultation logs and compile responses thematically for consideration by the Pilot Project team.
- The Corporate Lead and Divisional Lead and other selected Trust Reps will meet with individuals or groups, as practically possible, who have raised specific issues that should be incorporated into proposals and governing documentation in a co-design/co-production manner.
- On completion, the corporate and Divisional project leads along with the pilot project group (supported by Equality team) will consider all feedback received and will produce a response report for consultees and the Board on any mitigations and changes as necessary and a final proposal. This could include what forms the final content of the policy and procedure and privacy notice.
- Staff will be kept informed as the project progression via memos, newsletters, and updates to NHSCT website and SharePoint, via Trade Union colleagues etc. Staff will

be advised to raise any concerns immediately with either line management or a member of the project group.

How we developed our proposal and will consider our options

Pre-Consultation Engagement:

We engaged inclusively and constructively with our internal stakeholders to consider concerns, fears and misconceptions of those who work within our ED service and engaged with external stakeholders, including Trusts who have successfully implemented pilots and BWC use already to glean their experience, lessons learned and to identify any potential barriers and facilitators to feed into our planning. More, in drafting this proposal and associated pilot documents, the regional and trust strategic direction regarding the management and prevention of violence and aggression, research, best practice and the best interests of our staff have been thoroughly considered.

Reveal Media Ltd (BWC Supplier)

The Estates Rep and Divisional Governance Rep liaised with Reveal Media Ltd to ascertain what options were available to the Trust with the pilot package, costings and potential data models (hosted cloud vs on-Prem servers). Following receipt of this information the Sub-Group discussed the differences and costings for both models. It was decided that Cloud hosting would be best for the pilot given that the ICT team were heavily committed at the current time due to Encompass preparations and the cloud model was the most economical given the size of the pilot. However, the Group acknowledged it would possibly consider an on-Prem model should there be a much larger scale roll out at a later stage. An ICT Security & Technical survey was shared with the supplier for completion and the ICT Security Rep will liaise with the Supplier to close out any remaining queries and to provide assurance to the Trust that they are satisfied with the controls in place to adopt use of the technology. The supplier will also liaise with ICT colleagues near the time of setting up a pilot to ensure proxy and bandwidth requirements for data transfer and any other aspects are correct to enable a smooth transition for the pilot.

Networking with Regional Colleagues/Other Trusts (Northern Ireland)

Sub-Group members reached out to their colleagues (based in ICT, Information Governance, Equality, Projects and Services) in other Trusts within the region to glean what information and learning was available from their experience of piloting and implementing the use of BWC cameras. While it was known no ED in the region had piloted the intervention and it had been used in different settings, both NIAS and the SHSCT colleagues were very receptive, supportive and provided very valuable insight into their approach and understandings to-date. All of which has helped shape the Groups plans and the drafting of pilot documentation. Additionally, the Trust Data Protection Officer (who is also a Rep on the Sub-Group networked with one of the Information Commissioner's Office (ICO) Reps on regional IG Forums to make them aware of the Trust plans and initial considerations. Additionally, it was acknowledged the Trust have considered the ICO Guiding principles and number of other best practice/guidance documentation to inform its drafting, including the Surveillance Camera Commissioner checklist.

ED Nursing staff & Trade Union Support

Consultation and Trade Union Support (TUS) is considered key to helping staff understand the reasons for implementing this intervention and to allay any potential fears or misconceptions as to why BWC devices are being introduced. For this reason, the Trust engaged early with ED staff and TUS (RCN, UNISON & BMC) to ascertain initial/early viewpoints and with a recognition that the pilot, for some, could be interpreted as controversial and carrying risk of impacting negatively on the nurse-to-patient relationship. Yet, having engaged with both band 6 and band 7 Nursing Sisters (on 16/02/24) and with band 5 ED nursing staff (04/04/24) the sub-group Reps were not met with apprehension and staff were welcoming of the pilot ,viewing it as a signal of support from senior leadership. NIAS Reps kindly attended the latter session and provided a presentation of their BWC pilot

"successes". During these discussions with staff, there was opportunity to address initial queries staff held and this included whether participation in the pilot by nursing staff would be compulsory; whether all nursing staff would be wearing devices or just some on shift; whether BWC recordings reduced the need for staff to attend court to provide evidence following an assault; whether consent was needed to activate BWC recording; the potential for unintentional activation of devices; the need for accompanying policy/procedure and whether BWC use can help plug any potential gaps in CCTV surveillance. Reassurance was given to staff that participation at the current time will be discretionary and a discussion was had about the need for staff using BWC devices to feel comfortable, confident and competent in their use. Staff were advised there will only be a small number of devices for the pilot, resulting in a select few nurses wearing BWC during a shift. NIAS advised staff that in their experience having BWC footage has avoided the need for staff to attend evidence following an assault, but this does not negate the need for statements to be given to the PSNI following an event. More, NIAS highlighted that footage from BWC has been beneficial in resolving fictitious claims from service users involved in assaults by providing an independent account of what happened. That this has also significantly reduced the time necessary to investigate incidents which are recorded as video footage can be viewed without the need to chase context and information from the individual victim to the assault. Discussion included reference to the lawful basis of legitimate interests and an explanation as to why consent would not be practical in the context of how the devices are to be deployed. Staff were advised that any unintentional activation can be deleted and the Trust would have accompanying policy and procedure for use of the BWC devices and training on the same prior to go-live. Staff acknowledged the benefit of the BWC devices being portable given the belief that there could be "black spots" /gaps within many areas already covered by CCTV surveillance and sound recordings will provide additional context to what is going on. ED nursing staff had the opportunity to handle a deactivated Calla BWC device which was made available, without cost, by Reveal Media Ltd for information sessions. They also had the opportunity to handle the device currently utilized by NIAS. It was felt this was useful as an aid for staff to visualise the size of the device and feel the weight, which might spark practical considerations.

<u>Northern HSC Trust Key Internal Stakeholders (across divisions/departments)</u>
The Corporate Project Lead, Divisional Governance Lead and CSM for ED met with key internal stakeholders from both within ED and across the division and wider Trust services (on 05/08/24) to provide an update on the pilot. At this event a presentation was delivered with a Q&A thereafter. No concerns were raised throughout the session

<u>Engagement Advisory Board (EAB)</u>
The Divisional Governance Lead and Head of Equality delivered an oral overview about the outline pilot proposal at the February Engagement Advisory Board (EAB) (28/02/24) and thereafter held a question and answer session with EAB members. This provided an opportunity for good discourse. Members of the EAB held mixed views, but overall were in support of the introduction of the technology for the reasons detailed by Trust Reps as to the legitimate aims of the pilot i.e. BWC devices could be used as a deterrent to the acts of violence and aggression towards staff, patients and/or others. Members of the EAB raised a number of questions and these were noted and informed the development of a FAQ/Information leaflet, which will accompany the Consultation document. This included questions such as how will the Trust determine when BWC devices will be used; the footage would be good for staff training and learning; what happens data captured; what happens data accidentally captured and how many BWC devices will be in use?. The group also raised a number of other queries which form part of the considerations detailed within this DPIA document such as consideration of vulnerable groups (MH/DoL scenarios, children etc.) and how does the pilot connect with staff de-escalation training.

<u>Hospital Mental Capacity Act Lead</u>
The Divisional Governance Lead met with the MCA Lead (23/05/24) to discuss the proposed pilot, associated protocol and to consider any implications from a MCA and/or restrictive

practice position that need specific acknowledgement in operational protocol. MCA Lead of the opinion that BWC use in ED is not Deprivation of Liberty (DoL) as acid test/definition not met. More, use of BWC itself does to restrict individuals from leaving the environment so it cannot be considered restrictive practice (not impeding individual movement) and an individual under DOL will be under supervision anyway so BWC is not materially different. Only difference is the BWC is recording the interaction (independent view). MCA Lead of view that Human rights considerations (Arts 3&8) for potential recording of individuals with MH more applicable in considerations and that these have been addressed as part of the wider DPIA documentation. Reference made to ED environment and the potential for patients/public within ED environment having MH issues and this may be known/unknown to those in proximity. Reference made to capacity and not all MH patients will have capacity issues. Discussion regarding the transient nature of capacity at times – with some individuals lacking capacity due to alcohol/drug issues or delirium. Acknowledgement of more permanent capacity issues such as dementia. Confirmation lawful basis for use is not consent based/reliant on capacity itself, but legitimate interests. Akin to best interests.

Health & Safety Manager

The Divisional Governance Lead, H&S Manager and Assistant H&S Manager met (25/04/2024) to discuss activation criteria and proposal. Update provided on MCA Lead discussion and reference made to the unpredictability of ED in terms of identifying diagnosis/medical conditions of those present, if not being treated. Agreement that exclusion criteria based on capacity not necessary as operation based on legitimate interests/best interests of the "collective". Nevertheless, protocol for use of the technology should bear in mind characteristics of individuals and potential impact of use of the intervention and any action must be reasonable and proportionate. Agreement that BWC documents/activation SOP needs to be aligned to wording/language of the MOVA Framework. Activation wording/criteria updated to reflect that which is included in the HSE (2019) definition of work-place aggression and the MOVA Framework.

PSNI

The Divisional Governance Lead met with the PSNI Chief Superintendent for Northern Area and Belfast Area (14/06/24) to notify them of the Trusts proposal and stage in the planning process. Query raised with PSNI whether Trust need to consider anything further in terms of integrating with partnership working and alignment with evidence/forensic protocol. Discussion had regarding benefit of available BWC evidence for PSNI and Trust and in terms of reducing the likelihood of Trust staff having to attend court, though acknowledgement that written accompanying statements will still be a requirement.

NHS Trusts – England

The Divisional Governance Lead made contact with a number of English NHS Trusts in England who were identified as either piloting or implementing BWC devices within their ED(s) (*Nottingham, Gloucestershire, Bart's, and Bristol, the University Hospitals of Derby & Burton and University Hospitals Coventry & Warwickshire*). A number of supporting articles were gathered regarding these Trusts use of BWC devices and these can be found in the legitimate Interests Risk assessment, under research and evidence. To-date it has not been possible to meet with all of these English Trusts, but the Trust would hope to meet and continue to correspond with this national colleagues as engagement continues.

Established contact/meetings/correspondence to-date:

Nottingham University Hospitals NHS Trust

The Corporate Project Lead and Divisional Governance Lead met with the Associate Director of Operational Risk (22/05/24) to discuss their experience of introducing BWC within their ED and in other Areas. This feedback was highly complementary and the Trust was advised that while they did not see a reduction in the volume of incidents initially, they did see an increase in measured Psychological safety and staff indicated they felt support and listened to by senior management and the intervention was having a positive impact on

their wellbeing and job satisfaction as they were not having to invest so much time dealing with incidents/events.

Gloucestershire
Divisional Governance Lead in contact with the Head of Corporate Risk, Health & Safety (07/06/2024) who advised they are half way through a 3-month pilot in their ED. Nonetheless, to-date their Trust have been observing positive benefits from the intervention in relation to: Effective de-escalation of situations as the perpetrator is aware we are recording; Recording incidents for the purpose of evidence in relation to our Behaviour Standards Panel (issues warnings and sanctions to patients / public); Sharing with the police to support prosecutions, warnings, criminal damage, and injunctions; Helping staff to feel safer at work; Learning aspects in relation to our incidents and response. The Trust would hope to link back in with Gloucestershire when they are at their evaluation stage (as part of our consultation).

Other
A pre-pilot survey has been developed and will be conducted to further gauge staff attitudes and perceptions towards the technology, their level of understanding and to identify any concerns or needs that can be addressed through continued engagement and/or training. More, this survey will act as a baseline measure which will be compared with future data collected as part of the evaluation.

Full Consultation Stage
The purpose of this consultation is to engage widely in a conversation with our stakeholders that will fully consider all of the relevant perspectives and potential impacts of our proposal – in principle - to introduce Body-worn cameras for Trust staff. This will inform further work on assessing and finalising processes and in considering the impacts of such a decision. *The DPIA, LIA and all other documentation will be revisited following the consultation and amended, as necessary.

During the consultation period we will hold listening events. These events will be publicised and will provide the opportunity to ask further questions and give feedback. To facilitate public feedback, a consultation Proforma will be made available on the Trust. If stakeholders have any queries or comments regarding this consultation document, EQIA or RNIA or any other supporting draft pilot document and there availability in alternative formats (including Braille, disk and audio cassette and in minority languages to meet the needs of those who are not fluent in English) they will be able to contact the Equality Unit. In compliance with the legislation, when making any final decision the Trust will take into account the feedback received from this consultation process. A consultation feedback report will be published on the Trust website.

STEP 8. EVALUATE THE PROCESS	
Function creep is the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended as set out this DPIA, especially when this leads to potential invasion of privacy. Are you content with the measure in place that there is no risk of function creep?	**YES ☒**
The use of BWC devices for safety and security purposes has increased significantly over recent years as the technology advances in leaps and bounds and prices fall making them an affordable intervention/solution. Nonetheless, the Trust recognise the importance of controls being put in place for their use to avoid function creep. This is considered under the section 11, Risk assessment.	

This DPIA has been drafted with consultation with key internal and external stakeholders, including the NHSCT Data Protection Officer and will be revisited following the formal Public Consultation and/or later following deployment of the intervention should there be an operational requirement to alter how the technology is being utilised that extends beyond the defined scope.

Governing and Supporting Documents
A suite of policy, procedures and other resources, along with a training programme will be developed and provided to NHSCT staff using the technology to ensure scope of use, requirements and expectations are clearly defined and understood by staff and management associated with the pilot. Roles and Responsibilities of Trust staff will be set out clearly as part of policy.

Items under development includes:
- BWC Privacy Notice;
- BWC Signage/Posters;
- BWC Information Leaflet and Frequently Asked Questions;
- BWC Policy, within inclusion of Records Management Protocol ;
- BWC Standard Operating Procedure (SOP);
- Training programme for use of BWC devices and associated software (aligned to protocol, best practice and legislative considerations);
- Audit Proforma to monitor policy compliance.

The NHSCT website will be updated with these documents during the Public Consultation to enable members of the public to comment on content, alongside this DPIA, the Legitimate Interests Assessment, ICT Technical & Security Questionnaire and the Consultation Document. Following consultation, all feedback will be considered with a view to amend and improve the documentation, as necessary.

There will be two levels of training – BWC Operator and Administrator/Senior Nurse/Operational Manager. The latter will focus on administration of the associated video management software (DEMS-360). Both will be delivered by the supplier of the cameras, Reveal Media Ltd and will each last approximately 60-90 mins.

BWC Operator/ Initial Responder (IR)	• How are Body Cameras an effective deterrent • Why are we using BWC (Inc. attaching devices and activation criteria) • Camera features & functions (familiarity training) • Installation, setup and maintenance of BWC devices • Docking and software uploads • Best practice techniques and reference to principles of this document • Q&A
Administrator/ Senior Nurse/Operational Manager	• Reporting faults and damaged equipment; • Functionality of the video Management Software (DEMS-360) • Gaining access to the video management software (DEMS-360) • How to use software to utilise functionality (viewing, copying, labelling) • Accessing support • Q&A

In addition to specific training on the use and management of BWC devices and the administration of associated software, all staff involved in the pilot will be required to keep up-to-date with relevant Trust mandatory training on Information Governance and Records Management. All staff will also receive refresher training on 'First Response to Mental

Health' (*designed for any staff member who wishes to acquire or refresh their knowledge and skills of dealing with someone who is in emotional or mental distress*) and 'Mental Capacity Act Level 2 General Overview of Deprivation of Liberty' (*designated for staff who work in any setting where DoL may be required and in particular, those who will be involved in applying DoL processes/ procedures associated with the Act*).

BWC devices and associated software will be registered information assets and managed by the aligned Assistant Information Asset Owners (AIAOs), which involves definition need, use and any associated risk.

The Trust will only deploy BWC technology against the defined operational requirements and with governance around its use to ensure that use is proportionate, legitimate, necessary and justifiable. At all stages, the NHSCT will comply with the UK-GDPR and the Data Protection Act and other legislation such as Human Rights Act; there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim, as detailed.

Records Management
Back office software (DEMS-360) date stamps all recordings. Footage will be assigned to a Retention Policy as either "evidential" or "non-evidential" and by category of data held. Within the software these retention policies can be set up to ensure that footage is retained for the appropriate amount of time. Auto-deletion will be activated for when footage has reached the full duration of the retention policy it is assigned to. Once reached, it will filter itself out the DEMS 360 system. For example – "Non-evidential" footage can or will be set up to be automatically deleted after 28 days from the date of upload. Whilst "evidential" footage is retained for much longer periods, as set out in the retention schedule (and detailed in the privacy notice). The decision of when footage is evidential or not lies with the person that is authorised to view footage (Nurse Management). As with any incident, it will be recorded into Datix which will note that body worn camera footage is available to substantiate the events of the incident. Datix will also have a checklist field to enable reports to be run on Violence and Aggression incidents supported by BWC footage and this will inform the evaluation of the Pilot.

Access Management
As mentioned, Roles and Responsibilities of Trust staff will be set out clearly as part of policy and this too impacts internal access of collected data. The roles and associated/aligned access by role will act as a control and ensure access to data is restricted and on a need to know basis. Each BWC device will be password protected to prevent unauthorised viewing or amendment to the device's settings. The BWC devices have been specifically designed to have no playback feature on the physical device and footage is AES256 bit encrypted. When "Encryption" and "Trust Mode" are activated in the DEMS 360 software, this locks the cameras to the NHSCT DEMS-360 installation. This prevents any access to the footage outside of NHSCT DEMS-360 software. Specific PCs in proximity to the ED Sisters Office shall be configured to act as a DEMS client machines. These shall have camera unit docking stations attached to enable the auto-uploading of footage (with uploader support, users can only see status of uploads/charging). Once uploaded, the footage is automatically deleted from the device. Access to the DEMS-360 software is username and password protected and software user actions are auditable and logged. System Administrators are nominated by the Trust and are senior managers with appropriate level of authorisation and clearance within the Trust. The training provided by Reveal Media Ltd will provide a solid foundation for system administration.

What measures will be in place to ensure the accuracy and quality of the data being processed?

How BWC data is captured will comply with the requirements of UK-GDPR and the Information Commissioner's Office (ICO) Code of Practice. Trust staff will only activate

devices in line with set protocol for a legitimate purpose. The devices are capable of capturing quality images of a sufficient quality to allow individuals to be identified. This is something that will be monitored throughout the pilot as poor quality data may undermine the purpose for utilising the BWC surveillance in the first place. Following any activation, data will be docked and downloaded to reduce the risk of data held on device becoming corrupt/inaccessible and this has been built into the associated Standard Operating Procedure (SOP).

BWC footage will be stored in a way that maintains the integrity of the data, to ensure both its evidential value and to protect the rights of the individuals whose image or voice may have been recorded. Accordingly, access will be strictly limited. If footage is to be retained for evidential purposes, the designated person will produce a copy from the system and ensure it is stored securely and in line with the Trust's Forensic Readiness Policy, a record will be kept of the following: date on which the footage was removed from the BWC; reason it was removed; location of the footage and name of the person who removed it. Duplicate copies of data will either be held by creating an ISO file using the BWC software and burning this to a disc or via duplicate storage on a separate tenant of the cloud server. The method to secure BWC data will be auditable and audited regularly during the pilot.

The Pilot will be supported by Policy, SOP, FAQ, Privacy Notices, a bespoke training package and existing processes and controls adopted by the Trust to maintain quality and accuracy of data processed on servers.

The associated BWC Pilot Policy can be read in conjunction with a number of supporting Trust policies and related legislation.

- UK-GDPR
- Data Protection Act 2018
- Information Commissioner's Office (ICO) Guidance on Video Surveillance (including CCTV)
- Surveillance Camera Code of Practice
- Regulation of Investigatory Powers Act 2000
- DoH Good Management, Good Records (GMGR) 2017
- Retention and Disposal Schedule NHSCT/21/1572
- CCTV Surveillance Systems – NHSCT 23.1731
- Processing of Personal Information (POPI) - General Procedures – NHSCT 22.1703
- Making Information Available to the Public (MIAP) Procedures – NHSCT 22.1702
- Information Asset Owners and Information Asset Administrators Guidance – NHSCT 22.1655
- Portable Appliance Testing of Electrical Equipment Policy – NHSCT 18.1170
- ICT Security Policy – NHSCT 24.1908
- ICT Acceptable Use Policy – NHSCT 24.1909
- Adverse Incidents Reporting and Management – NHSCT 211570
- Complaints and Service User Feedback Policy and Procedure – NHSCT 24.1927
- Management of Violence & Aggression Framework/Toolkit vers.2 (March 2022)
- Restrictive Physical Interventions – NHSCT 24.1879
- Operational Guidance to Support the Implementation of the Mental Capacity Act (NI) 2016 (MCA) Deprivation of Liberty Safeguards (DOLS) 2019. – NHSCT 24.1882
- Acutely Disturbed Behaviour, Management Through Pharmacological De-escalation & Rapid Tranquilisation – NHSCT 23.1790
- Forensic Readiness Policy – NHSCT 23.1768
- Liaison and Effective Communications with the Police Service of Northern Ireland (PSNI), Coroners Service for Northern Ireland and the Health & Safety Executive Northern Ireland (HSENI) when Investigating Patient Safety Incidents Involving Unexpected Death and Serious Untoward Harm – NHSCT22.1628
- Recording and Audio Devices within Northern Health and Social Care Trust Facilities; Guidance for Use – NHSCT 24.1914

- NHSCT Patient and Service Users Privacy Notice
- NHSCT BWC Pilot Privacy Notice
- NHSCT Staff Privacy Notice

What measures will be in place to ensure the data minimisation principle is adhered to? *I.e. only processing or sharing what is necessary and the minimum amount needed for the purpose.*

Associated BWC data collection pilot forms (located in the Policy appendices) make use of pre-set data fields to ensure no more information is collected than necessary.

The Trust recognises that Data Protection legislation requires that information that can identify an individual is not kept for longer than is necessary. The Information Commissioner's Office (ICO) Code of Practice further states that CCTV/BWC footage should only be kept for the minimum period required to serve the purpose. Accordingly, BWC device data will be retained for 28 days, in line with the Trust's Retention and Disposal Schedule and Department of Health (DoH) Good Management, Good Records Disposal Schedule 2017 (last updated 18 May 2022), unless there is a statutory or legal requirement to retain for longer than the specified retention period i.e. complaints or legal proceedings. Automatic erasure or overwriting of the data (using software functionality/parameters for data retention) will take place to ensure this time-scale for retention is strictly adhered to.

Retention periods for BWC device data are:

- Data captured due to accidental activation and/or training will be marked for immediate deletion.
- Data not marked for retention or where there has been no Subject Access Request, Incident or Complaint, will automatically delete after 28 calendar days (as aligned to purge of CCTV data from Trust servers).
- Data relating to an adverse incident (A2 & Evidence under N1) or Complaint (B2) will be retained for 10 years from date of last action.
- Data relating to a serious adverse incident (A4) will be retained for 20 years from date of last action.

Where an incident has resulted in litigation, records relating to the litigation will be managed as per GMGR Section on litigation (I1). Records will be maintained for 6 years from the date of the last action on the file or settlement of the case, whichever is the later and as advised by legal advisors. NB: cases where the proceedings relate to a minor (i.e. anyone under the age of 18) records should be maintained until their 25th birthday. In cases involving a person under a disability (see definition in GMGR, Part 1) records should be retained.

When it is deemed there are valuable lessons for wider team learning and development around the de-escalation of aggression and violence, BWC data may be held separately and retained for training and education purposes. In such circumstances, data will be held for a period of 8 years following the delivery of the training (J58) and the identity of the subjects captured will be masked, where possible.

STEP 9. CONSIDERATION OF DATA SUBJECTS RIGHTS

1. Right to be informed

Is the project covered by an existing privacy notice? A bespoke privacy notice has been developed for the BWC pilot. This sets out an introduction to the pilot, contact information for the data controller, Data Protection Officer (DPO) and Information Commissioner's Office (ICO), the purpose and lawful basis for processing data as well as retention schedule and individuals rights.	**NO** ☒

The BWC pilot privacy notice will be made available in a range of formats. Notably, it will be available digitally via scanning QR code on ED signage/posters or in the FAQ/Information leaflet or via access on the Trust website and a hard copy will be available at ED reception. Other formats can be made available on demand. Staff, as part of their training, will be made aware of this and all other supporting resources so they are adequately prepared should members of the public or patients have queries.	
2. Right of access	
The organisation is obliged to provide personal information upon request in line with Data Protection Act 2018 and UK GDPR. Have you considered how this will be achieved in your project? Please provide details below: The Trust has existing mechanisms and process embedded for the management of requests in line with Data Protection legislation. This pilot will adopt these same systems and acknowledgement to these processes is made in documentation associated with the BWC Pilot, such as the Privacy Notice, Policy document, FAQ.	**YES ☒**

STEP 10. PERSONAL INFORMATION SHARING AGREEMENTS	
Is there or will there be a <u>contract</u> in place containing specific data protection clauses* with the organisation(s) you plan to share information with? **** the contract clauses will need to reflect the mitigations identified at Step11 to minimise the data protection risks*** Licence agreement (DSA) will be in place with Reveal Media Ltd for a Cloud Hosted Solution using BWC software solution/package (DEMS-360).	**YES ☒**
If NO, in the absence of a contract what agreement will be in place? ***e.g. Data Sharing Agreement, Data Access Agreement, Memorandum of Understanding*** **Please provide details below:** N/A	

Step 11. IDENTIFY, ASSESS AND MITIGATE ANY DATA PROTECTION RISKS

In this section you are asked to first identify and describe the specific risks associated with this project/process and assess the nature of potential impact on individuals. You will then describe the measures you could take to reduce each identified risk.

The **HSC Regional Risk Matrix and Regional Impact Table below** will also help you to assess the level of risk.

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant (1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Likely (4)	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Possible (3)	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely (2)	**Low**	**Low**	**Medium**	**High**	**High**
Rare (1)	**Low**	**Low**	**Medium**	**High**	**High**

Identify and Assess Risks				Mitigate Risks		
Describe below any specific data protection risks and nature of potential impact on individuals.	**Likelihood of occurrence** 1. Rare 2. Unlikely 3. Possible 4. Likely 5. Almost Certain	**Severity of harm+ (if occurred)** 1. Insignificant 2. Minor 3. Moderate 4. Major 5. Catastrophic	**Overall risk** 1. Low 2. Medium 3. High 4. Extreme	**List the various controls that have been or will be put in place to mitigate the risk prior to commencement.** **PLEASE ENSURE YOUR MITIGATION ADDRESSES THE RISK**	**Effect on risk** Reduced Accepted	**Residual risk** Low Medium High
Equipment failure/ Malfunction and Loss of Footage	33	22	22	BWC devices will be purchased in new condition and periodically serviced or as necessary. Equipment will be installed and maintained as per manufacturer's instructions and ward managers, as part of routine business, will check devices pre and post docking to ensure they are functioning and charged to a usable level. This will be incorporated in the BWC training, the SOP and subsequent policy. Any device issues / failures /damage/ incidents will reported via DATIX and investigated through liaison with ICT and the device supplier. Contingency replacement will be covered under contract with view to have any non-functioning or damaged devices replaced within a 1-2 day period, following return, to minimise potential downtime and reduced recording capacity. Should a device malfunction, there is still the ability for the device to be repaired or for data stored internally to be extracted. Should this not	Reduced	Low

				be possible in extreme cases, the greatest amount of data that could potentially be lost would relate to one incident only due to a policy on docking devices after each incident. All BWC data, both on device and on cloud server, will be encrypted. Data on server will be managed in accordance with retention schedules and data retention will be informed by coding inputted by senior managers who will review footage after each activation. Server data will also be backed up. All staff involved in the piloting of devices will receive specific face-to-face/ on site BWC training and will be expected to be up-to-date in ICT security and IG mandatory training. Training will cover practical use of the devices as well as maintenance, security, how to report faults and how to use the associated software (DEMs-360). Where multiple BWC Operators/IRs are present at an incident, all will record. This will reduce the impact of data loss should one device fail.		
Loss/theft of device	33	22	22	A small number of BWC devices will be deployed in each ED area of the pilot and devices will only be used by a select number of senior and experienced nursing staff operating within a small ED footfall. Each device in use will be tagged and asset managed with signed out/in protocol adopted by the staff members selected to use BWC devices. This process will be addressed in both training and the SOP. Additionally, the sign out/in register	Reduced	Low

				will be monitored by local ward management through routine checks and is auditable. BWC devices will not be worn outside of the ED. When devices are not located on staff operators they will be placed in a secure designated location within the ED. BWC devices when deployed will be securely attached to nursing staff uniforms and while there is possibility that a device could become detached due to a poor initial attachment, staff knocking off other objects or through a physical altercation, it is probable the device would be located within a short space of time, if not noticed at time of detachment, due to the volume of ED staff operating within proximity. Should a device become detached by force and/or stolen and fall into the possession of an unauthorised individual, the probability of said individual being able to access the data is considered very remote due to AES258 encryption of data held on devices and the requirement to dock and access day through licenced software. This will minimise the likelihood of any impact from data loss /breach. Risk of data loss and claims as a result are assessed as minimal give the procedural controls in place for device management, use and security of data (encryption, no access on BWC device itself, login required to access associated software and access only permitted to a limited number of senior staff).		

Holding excessive recordings due to inappropriate or continuous recording or poor policy compliance	33	33	33	BWC device default set up will not include continuous recording and protocol for operation will stipulate recording by activation. Likelihood of inappropriate use/recording will be minimised by the use of defined operational protocol on use and justification for use of the BWC devices and activation is covered within the DPIA. Activation will be considered a last resort. Any BWC device activated by a member of staff will be returned for docking and upload to the server following deactivation. A Datix report will be made following any activation relating to an incident and will make reference to the BWC footage existing and reason for activation. Datix reports will not be made for any accidental/ false activations. However, as part of the pilot evaluation ward managers will monitor the volume of these as it will inform future training need assessment and content. Ward Management already routinely receive Datix notifications and this will act as a safety net for the need to code the category of the data on the associated BWC software to prevent data loss. Ward Management, as part of normal business, will review BWC footage on a daily basis and/or following docking and will apply relevant category coding on the associated software. Data left encoded will purge from the system after 28 days, but this is intentional and will promote compliance with the data minimisation principle.	Reduced	Medium

				The system retention periods based on category coding will be informed by existing regional/DoH retention schedules used by all HSCNI Trusts. Data with multiple purposes will be duplicated and coded respectively e.g. SAI and Evidence for PPS. Any public body third parties receiving data will have a legal duty to manage and protect the security of the data within their own set timeframes for retention (i.e. DoJ schedules). All staff involved in the piloting of devices will receive specific face-to-face/ on site BWC training, will be expected to be up-to-date in ICT security and IG mandatory training and will have access to policy and procedure. Training delivered will cover practical use of BWC devices and engagement with patients/visitors, as well as maintenance and asset management (Inc. fault reporting), security, legislative considerations (e.g. HRA and DPA/GDPR) and for managers, use of the associated software. The associated software will have the ability to edit footage length and/or obscure sections of recording e.g. by applying masking of 3rd parties minimising any collateral intrusion. Privacy concerns will be a consideration should BWC data be requested and each request will be considered by the Trust on a case-by-case basis. Periodic audits will be conducted to evaluate policy compliance and to inform future training needs and content.		

				Data within the evidential category which has been passed to PSNI, courts etc. will be reviewed and disposed of, in accordance with timeframes within the justice system.		
Unauthorised copying of footage to personal devices(s)	33	33	33	Only devices issued by the NHSCT are to be used. This is set out within the Trust policy and SOP documentation. Data held on BWC device internal memory is encrypted to AES256 standard and cannot be viewed, edited or deleted on device. Data is automatically transferred to a secure server once the BWC device is docked and data on the device is purged. Data on the service can only be accessed by use of associated software and access to this software is limited to a select few senior managers associated with the ward area/division management. Use of the software can be reviewed through a system created audit trail.	Reduced	low
Server failure or shutdown due to fire, flood, viruses, other.	3	4	3	The suppliers hosting the services will monitor services regularly and proactively. Monitoring will help detect and resolve issues before they escalate into major problems and will have disaster recovery protocols in place. While the Server is Cloud hosted, the suppliers of the hosted servers will have controls in place to protect against risk of fire or flood damage to the physical services in data centres. However, commonly servers are based in multiple locations and data is routinely backed up daily. In extreme cases, it is likely the most data that could be lost would be restricted to the period of time from failure incident to time of last back-up,	Reduced	Medium

				provided servers remain intact or located in another setting (in context of fire/flood). Contingencies are in place (cloud exit plan) should the supplier organisation/subcontractors go out of business. At termination or expiry of a contract with Reveal, customers may either download their data themselves or request Reveal to retrieve the data from the cloud environment and provide this data to the customer (Trust).		
Function creep resulting in non-compliance with legislation and bringing potential for fines	33	33	33	DPIA drafted with local engagement and consultation with both internal and external stakeholders. The document will be revisited following formal Public Consultation and/or later following deployment as necessary. Scope of use of the BWC Devices will be defined by operational protocol and governing documents. All of which will have consideration of applicable legislation and best practice. Document references will be made available at time of Public Consultation and on demand during the pilot. Training will also be provided to all staff involved in the pilot. There will also be a requirement for these staff to be compliant in existing Trust mandatory training related to MHA/DoL, IG and ICT Security. Posters/Signage will be visible within the ED/areas involved in the pilot and a press release will be given prior to go-live/as part of	Reduced	Medium

				Public Consultation to increase public awareness of the pilot and Trust considerations. Audits will periodically be undertaken to monitor policy compliance.		
Contra-indication to use by patient and/or visitor responding adversely to use of the camera.	3	2	2	Consideration to this will be given as part of the strategies deployed by staff re: PMVA and BWC. Ultimately, staff will remove themselves if dynamic risk assessment suggests there is an active threat to their safety. This will be monitored throughout the pilot and Datix reports will inform monitoring and the post-pilot evaluation.	Reduced	Low
Increased costs associated with the use of equipment, management of software impacting on service budget.	3	2	2	A corporate budget has been deployed for the BWC pilot and this will not impact service budget at this current time. Furthermore, the cost of the pilot pack has been subsided by the supplier for the purposes of trail use. Cost-benefit considerations will form part of the pilot. While research suggests that costs can be offset against the benefits of having BWC devices in operation, it is acknowledged this may be difficult to measure in monetary terms during the pilot. However, benefits will be acknowledged in the post-evaluation and the use of the technology. Costing models will be considered should the pilot be successful and further roll out is approved by the Trust. This is involve consideration of data models/infrastructure, ownership of technology and data within the Trust etc.	Reduced	Low

				The Project Group for the pilot, in its consideration, decided that a hosted solution should be adopted due to cost efficiencies given the size of the pilot and given the existing commitments and capacity demands on existing Trust ICT resources due to Encompass Go-Live preparation.		
Increase in formal complaints regarding the use of BWC devices in the absence of consent	3	2	2	Consent is only one lawful basis for processing data under data protection legislation. This is set out within the context of the DPIA. The Trust will engage in a 14 week Public Consultation with all key stakeholders and will make available all project documentation, included the documented lawful basis for processing data while using BWC devices. This will provide all parties with an opportunity to seek additional information or raise concerns and the Trust an opportunity to give this consideration and respond prior to pilot go-live.	Reduced	Low
Demands for Freedom of Information and Subject Access Requests will increase and this could impact existing capacity to handle such requests and the timeliness of	3	2	2	The Trust are statutory bound to consider subject access requests received and has existing mechanisms for the handling and reporting on the handling of subject access requests. As part of early engagement for this pilot, the Trust consulted other Trusts currently using BWC devices and this suggested there has been minimal requests received by other Trusts following deployment of this new technology; nothing that would have material impact on capacity or require an additional resource need. Issues would as normal practice be escalated via senior management and consideration of	Reduced	Low

responses/legislative compliance regarding the same.				resources to meet capacity driven by demand would form normal corporate and divisional business. Volume of requests will be subject monthly monitoring within the division and will feed into the post-pilot evaluation.		
Measures taken against individuals as a result of the Trust collecting information about them might be seen as excessive or intrusive and potentially damage Trust Reputation.	3	2	2	BWC devices will primarily be deployed as a deterrent and they will used in a fair, just and proportion manner. Trust staff will be educated and trained in de-escalation tactics and will make all effort to deescalate a situation through deployment of strategies prior to activating a BWC. What an individual does thereafter is not within the staff member's control. It is not the Trusts purpose to take measures and it is not the basis for use of the BWC devices. Nonetheless, It is acknowledged that data may be requested by PSNI/PPS investigating incidents/inappropriate behaviour, public disturbances or criminal acts. The Trust as employers have a statutory duty to protect the health and safety of its staff. The Trust also has a duty to care for those patients in its care and to ensure safety of those visiting its premises. This should be something balanced in public interest when considering any potential impact of measures taken against an individual as a result of PSNI/PPS use of BWC footage captured by Trust staff.	Reduced	Low
Proximity and vantage point of BWC	3	2	2	The BWC devices will have a wide-angle vantage point. Privacy notices and posters will be on display within the ED to alert members of the	Reduced	Low

cameras may increase level of privacy intrusion and potential to capture footage showing 3rd parties and individuals in distressed state.				public and patients of the use of devices and staff present can answer any initial queries. Training will be deployed to all staff selected for involvement in the pilot and the BWC devices will only be used in 4 areas of the ED within the Antrim Area Hospital site. Training will include considerations of privacy, data protection and individual's human rights and operational protocol will determine use of the devices. All of which should minimise the impact on any individuals captured by the devices when deployed. Access to the data on servers will be limited to a select few senior management and the associated software used to view footage has masking/redaction tools that can protect the identity/privacy of 3rd parties should data need to be released. Information Governance and Equality expertise sought on an ongoing basis. As part of the DPIA a stakeholder analysis was conducted and consultation with key stakeholders has informed the Trust's review. Full Public Consultation will be carried out and this will include the disclosure of policy and governing documents associated with the pilot. The consultation will also include a number of public engagement events where there will be an opportunity for questions and answers, which should bring a further degree of transparency on pilot process and aims.		

				During the pilot, the privacy notice will be made available for public. BWC assets added to Trust information asset register. This will involve Asset tagging of BWC devices and maintenance plans in accordance with manufacture instructions.		
Staff mistrust about use of BWC if purpose not clear which could impact on staff-management relationships and be seen as unjustified intrusion.	3	2	2	The pilot project group have engaged with internal key stakeholders and ED staff at all grades. No concerns have been raised to-date by staff and conversely, ED staff have been welcoming of the pilot. Trust engaged with ED nursing management and staff at an early stage of preparation to make clear initial consideration and the purpose of the proposal to pilot the use of BWC devices. Made clear to staff that purpose does not include monitoring of nursing duties or view to appraise staff. Trust pilot project group also had early engagement with TUS colleagues to ensure they were informed of the Trust considerations and direction of travel should they receive queries from members. Trust pilot project group were monitoring feedback that come from staff during early engagement events and will continue to monitor feedback throughout the Public Consultation and will respond accordingly to ensure any concerns are alleviated and queries addressed.	Reduced	Low

Step 12. SIGN OFF and record outcomes

a. <u>Project Lead / Service Lead</u>: In signing this DPIA I confirm the following:

I am satisfied that this is an accurate reflection of how the service will be provided and the expected data flows. I have consulted with all necessary stakeholders and sought the views of others as required (including IG and ICT). I have incorporated relevant advice into this document and into the plans for delivery of the service. Where necessary, I will ensure any additional documentation is put in place, such as a Privacy Notice to inform service users of how their personal data is to be processed; and/or any required Contracts or Agreements to cover data sharing with third party organisations.). I will ensure the contract or alternative information sharing agreement will contain specific data protection clauses which address the risks identified.

I confirm that I will keep the DPIA under review and will update this document with any substantive changes to the data processing activities or data flows.

Any additional comments:

This DPIA will be kept under review and amended, as necessary.
Presently,

- Ongoing monitoring of consultation.
- Mitigations accepted and will be implemented.
- Any necessary contract/data sharing agreements will be put in place
- Policy/Governing documents will be in place and approved prior to any pilot go-live

Name and Job Title: Edward M. Smyth, Divisional Governance Lead (MEM)

Signature: E. Smyth	**Date:** 10/01/2025

b. Data Protection Officer (DPO) advice and sign-off

Summary of DPO advice:

- Staff should receive the appropriate training in the use of the camera and any SOPs developed to ensure they are aware of the measures to be taken when the recording commences.
- Privacy information should be shared appropriately and any posters displayed in the relevant public areas to ensure the Trust complies with its requirement to inform service users / staff and the public that recording could take place.
- Staff should have up to date Corporate Mandatory Training in Information Governance and be aware of their duty of confidentiality.
- The processes for the destruction of recording should be monitored to ensure compliance with the retention periods and assurance

Name: Neil Martin, Director, Strategic Planning and Performance Management

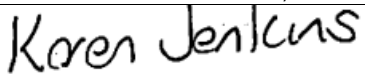
Signature: 	**Date**: 14.01.2025

c. Information Asset Owner (IAO) - Final Approval

I have considered the data protection aspects of this project and any DPO comments (above). I accept any residual risks and will ensure the various controls outlined to mitigate the identified risks are put in place prior to commencement. I will ensure that no data processing will take place until this DPIA has been completed and signed. I will ensure that this DPIA is reviewed and updated if the data processing changes. I will ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training. I will arrange for this new system/process to be added to the Information Asset Register (IAR) and/or Risk Register.

Any additional comments:

Name and Job Title: Karen Jenkins, Divisional Nurse & Governance Manager (AD)

Signature: 	**Date**: 14.01.2025

Additional: Examples of possible risks

Elements of risk mitigation, covered within the Governance of this BWC pilot and existing Trust processes, have been highlighted below

DP Principle (see App 1)	*Example Risks*	*Example Mitigations*
Lawfulness, Fairness and Transparency	Inadequate Communication – individuals not informed of how the HSC organisation will use their data The form of processing may raise public concerns (e.g. using CCTV footage/audio recording function without informing staff/service users) Privacy notice, consent form, policies and processes not sufficient to cover lawful basis	Privacy Notice in place
		Staff and service users will be informed of the method of data collection and how the data is processed i.e. CCTV/audio recording notification
		Standard operating procedures/staff guidance/ HSC organisation or regional policy/privacy notices and consent forms to be drafted or reviewed in line with the project outcomes
Purpose Limitation	Risk of function creep – that the data is used for a purpose other than the one specified such as using data collected for health for targeted marketing purposes Third party processors/contractors using data for purpose not specified (e.g. marketing purposes)	Clearly defined purpose and limitations set out in information sharing agreement/contract. Review of internal SOP.
		Clearly defined roles and responsibilities included within Contract/Information Sharing Agreement
Data Minimisation	Collecting more data than is required to fulfil purpose	Use of pre-set data fields to ensure no information is collected than necessary
Accuracy:	Mechanisms not in place to ensure data quality/ accuracy to avoid an unintentional data breach or non-compliance.	Ensure all procedures and agreements around data checking are fit for purpose.
	Inappropriate linking/merging records	• Understanding whether system has capacity to link records and if this is appropriate • Ensure there are Data Quality policies and procedures in place
Storage Limitation	Retention – information being retained longer than necessary	• Standard operating procedures to be drafted or reviewed in line with Good Management/ Good Records • Ensure that data retention periods (reflective of GMGR) are outlined in contracts and information sharing agreements and mechanisms exist to manage this by the appropriate parties
	Personal information (manual and electronic records) held with no formal retention policy in place	• Standard operating procedures to be drafted or reviewed in line with Good Management/ Good Records • Ensure that appropriate procedures are in place for retention and disposal of these records
Integrity and Confidentiality (Security)	Risk from threat actors such as cyber criminals, hackers or disgruntled employees on system or cloud	• Use of suitably secure network and file transfer system for transferring information between organisations i.e. Egress. • Consultation with ICT Security re system security. Timely removal of access
	Cyber-attack from unknown source received into the HSC organisation (e.g. opening attachment from unknown source which may contain virus)	Consultation with ICT Security team regarding data flows to asses network or system vulnerabilities
	Use of HSC organisation apps on personal devices without a known level of security	Consultation with ICT Security team regarding app/usage vulnerabilities
	Risk when transferring information internally or externally that the information could be inappropriately disclosed during transfer due to inadequate control	**N/A – File Share Platform to be used.** Information transferred in line with the HSC organisation's Email Policy i.e. use of secure file transfer system/password protected or encrypted emails
	Unauthorised access to information	• Consultation with ICT Security team re data flows to asses network or system vulnerabilities • Contracts/network access agreements in place • Regular review of systems access holders and prompt removal of access for those no longer requiring it
	Inadequate redaction/anonymisation of data	Checks to be completed on all anonymised/redacted data
	Loss of information due to inadequate controls around tracking/retrieval	• Adhering to data protection policy/guidance • Complying with UKGDPR and Good Management, Good Records to ensure appropriate measures in place to track and retrieve physical documents
	International transfers not monitored resulting information being transferred to servers based in countries without adequacy status or similar DP regime to UK/EU	**N/A** • Consultation with ICT Security team to identify location of servers and ensure appropriate

		controls are in place if information will be held in servers outside EEA • Contracts/information sharing agreements will contain clauses governing the transfer of data outside the EEA
	Data loss risk due to system failure	• Back up policies in place for ICT • Business continuity measures assessed and in place • Contracts/information sharing agreements to contain clauses governing data loss by 3rd parties
	Intended or accidental linking of data sets that may result in anonymised or pseudonymised data becoming personally identifiable.	• Understanding of whether system has capacity to link records/whether this is appropriate • Data Quality policies and procedures in place
Accountability	Receiving organisation having inadequate framework to support data protection	Assurances to be provided by receiving organisation in the terms of the contract.
CCTV/BWC Risks	New surveillance methods may be an unjustified intrusion on privacy	Identify appropriate lawful basis and consult ICO if required to ensure data collection is justified
	Vulnerable people may be particularly concerned about the risks of identification	Appropriate privacy notice in place
	CCTV system is not used for its specified purpose.	• Purpose clearly specified in DPIA/Public Notices • Access to footage limited to only those who require it • Signage in place
	Inability to exercise information rights (e.g. SAR, FOI) if system does not have the functionality to pixelate images which are not the subject.	• Ensure that any surveillance product has the functionality to pixelate or that appropriate contract is in place for ad-hoc pixilation with a third party company • Ensure appropriate surveillance policies and processes are in place and that any action taken is compliant
Data Protection Training is mandatory for every member of HSC staff and should be completed at least every 3 years. Data Protection training will reduce the risks to organisations for non-compliance of UK GDPR and should be considered as an additional mitigating measure for the above mentioned risks.		

Appendix 1

Northern Health and Social Care Trust

Legitimate Interests Assessment (LIA)

This legitimate interest's assessment (LIA) template is designed to help you to decide whether or not the legitimate interests' basis is likely to apply to your processing. It should be used alongside our legitimate interests' guidance.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

Why do you want to process the data?

The Trust wants to process data captured from nursing staff wearing Body Worn Camera (BWC) devices with the main aims of this initiative being to:

- Protect and enhance the experience of patients, staff and others who access the ED unit by helping provide a safer and calmer environment for;
- Enhance the security and the protection of Trust property/assets;
- Influence behaviour by acting as a deterrent to acts of violence and aggression and aid to de-escalate of situations should they arise;
- Enhance staff education and learning on Management and Prevention of Aggression;
- Record an independent account of what happened should adverse events arise and have footage captured with evidential value to any review or investigative process;
- Support relevant authorities in the apprehension and prosecution of offenders by enhancing the type and quality of discoverable evidence should criminal or civil action be brought.

What benefit do you expect to get from the processing?

- The primary benefit from processing is the promotion of patient and staff safety within the ED pilot areas and supporting our staff.
- While it is anticipated that there may not be a reduction in the volume of adverse incidents initially, it is believed the BWC devices will have influence on the severity of the incidents which occur.
- It is hoped this in turn will increase psychological safety at work and help bolster staff morale and satisfaction by making real and perceived improvements to healthcare environments. It should also bring the public some assurance that there are safety mechanisms adopted in the vicinity.
- It is hoped BWC device use will deliver cost savings (directly or indirectly), reducing the actual and associated costs of violence and aggression incurred.
- It is expected the BWC will influence behaviour by acting as a deterrent and aid in the de-escalation of situations.
- The processing of the data will provide an independent account of events with the capture of audio and video data. This will provide clarity within any review or investigative process and potentially significantly reduce the time spent in investigation of events or complaints to reach a conclusion.
- In some instances this may result in staff being able to continue, resume or return to work in a timelier manner when they were subject to any issue or review.
- Where a complaint has been logged with police, footage can be made available and this should provide clarity for the police investigation in addition to staff statements. There is

also a possibility that the availability of BWC evidence may negate the need for staff to attend court, which should lessen impact on staffing capacity and emotionally for staff.
- There is also a benefit in the reviewing of BWC footage which can shape and influence staff education and reflective practice.

Do any third parties benefit from the processing?
Data subjects benefit for the transparency of the data obtained. When activated the data from the BWC will provide an objective account of an event with both visual and audio recordings. Third parties such as the police may also benefit from the availability of footage that can be requested to inform police investigations. However, as per existing Trust protocol, all requests from third parties will be considered on case-by-case basis with consideration of impact on individuals and balancing of wider public interest.

Are there any wider public benefits to the processing?
The Trust, its public reputation of transparency and accountability (for staff and those recorded) and the vital interests of the public will benefit from this processing. When there is a criminal matter under investigation the investigation staff and the Public benefit from this independent transparent account of events. Additional wider public benefit is clarity in review and investigation processed and anticipated quality of care benefit and cost-effectiveness from a reduction in absenteeism of staff which impacts on public budgets.

How important are the benefits that you have identified?
Very. Any initiative which may have a role in the enhancement of patient and staff safety, protection of health care property and accountability to the public will have significant benefits. Given the increasing volume and frequency of violence and aggression against healthcare staff it is important that the Trust respond appropriately to support and protect our staff and the public while receiving care. The benefit of transparent objective evidence of an event is vital to any review process and actions that can be taken to minimise harm or prevent a reoccurrence.

What would the impact be if you couldn't go ahead with the processing?
Data from Datix entries indicates a significant percentage of incidences of adverse behaviour between patients and towards health care staff; this can be in the form of physical, verbal, psychological, sexual or racial abuse. If the Trust is not able to process BWC data there is limited deterrent interventions at our disposal to respond to such behaviours. This intervention is one of many as part of the wider regionally adopted MOVA toolkit.

Incidences of restraint recorded on the BWC will provide an objective account of the incident and can be reviewed to determine the manner of engagement and to review potential to enhance practice and safety for all involved. If not able to go ahead with the processing the ability to confidently review such engagements is limited.

Incidences where there is damage or criminal activity to Trust property would have a significantly limited potential to be effectively investigated and the matter taken before the courts.

The processing of data collected will enable learning with the aim to enhance safety for all, professional practice, accountability and objectivity.

Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)?
Yes. Profiling of data will not be taking place with the introduction of BWC devices within the Trust/ED.

Are you complying with other relevant laws?
There will be compliance with Data Protection Legislation - the UK-GDPR 2018 and the seven key principles: Lawfulness, fairness and transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity and confidentiality (security) and Accountability. There will also be adherence to the Trust/Regional Records Retention and Disposal Schedule – Good Management, Good Records 2017; Data Protection Act 2018, Freedom of Information Act 2000 and the European Convention of Human Rights (ECHR) incorporated into UK law by the enactment of the Human Rights Act 1998; Information Commissioner's Office (ICO) and Security Camera Commissioner (SCC) Good Practice Guidance and PACE (NI) Order 1989 and Investigatory Powers Act 2000 for police investigations, if required, have also been considered.

Are you complying with industry guidelines or codes of practice?
Yes, consideration given to available Information Commissioner's Office (ICO) Guidance, British Human Rights Institute guidance on use of BWC devices, Security Camera Commissioner (SCC) best practice guidelines and the Department of Health Retention Schedules, MOVA Framework (& with consideration of B0319 Violence Prevention Reduction Standards and B0989 NHS violence prevention and reduction standard guidance notes).

Are there any other ethical issues with the processing?
As the BWC's are to be used within the Antrim Emergency Department (ED) setting there is cognizance of potential ethical issues of consent, insight and privacy in the collection and processing of personal data. Lawful basis applied has been given significant consideration and consent is deemed not appropriate or practical. There may be occasion when additional sensitivity is required by staff using the camera when in an area where a patient may be in a position of incomplete dress. The need to activate a camera in this situation will be on the basis of necessity to achieve the legitimate aim of the Trust which to enhance the security and safety of all within the unit. A detailed Standard Operating Procedure (SOP) and training will be developed to assist staff in operational use of the BWC and the Trust compliance guidance to activation, notification, use and recording will be monitored. Professional Judgement will inform activation and de-activation.

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

Will this processing actually help you achieve your purpose?
There is a growing body of evidence and research now to signal BWC devices are a viable intervention that can bring benefits and achieve purpose of deterrence. The Trust have engaged with NI colleagues in Trusts who have already adopted the use of BWC devices (NIAS and SHSCT) who report positive responses and outcomes to-date. Additionally, the Trust as part of pre-consultation engagement made contact with a number of Trusts in England. There is a growing number of EDs in England currently using BWC technology successfully. Trusts are finding staff feel supported and the devices act as a deterrent to those who are aware of their actions to modify their behaviours appropriately.

Is the processing proportionate to that purpose?
The processing is considered proportionate to the purpose and expected outcomes. There are no other identified alternatives to achieve the legitimate aim of this pilot. The proposal for the processing of personal data has involved consideration of the views of representation from the Engagement Advisory Board (a NHSCT Public/Service User Representative Forum).

Can you achieve the same purpose without the processing?
No. The purpose of promoting safety, transparency, accountability, deterrent to negative events, prevention of harmful or criminal acts cannot be achieved without the processing of data captured by BWC devices.

Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?
No. The recording of data will be for the least period necessary to manage a situation and ensure resolution to a state of stability, security and safety of all present. Fundamentally, processing will be undertaken on the principles of necessity and purpose limitation, proportionality and data minimisation and in accordance with Trust policy and related legislation. Data will only be processed if there is necessity to do so and in compliance with storage limitation will only be retained for as long as is necessary in compliance with GMGR 2017. The BWC device has a front facing screen ensuring there is obvious recording of the data subject. All aspects of data collection, review, storage has been considered by the Trust when designing the pilot.

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail. - ***DPIA Completed**

Nature of the personal data

Is it special category data or criminal offence data?
Article 9 UK-GDPR data/lawful basis is not a focus or defined data element for collection within this pilot. Article 6 UK-GDPR personal data will be collected within a healthcare setting. This is referenced within the aligned DPIA; depending on types of conversations/information volunteered in proximity while BWC devices are operating, there is possibility that special category data may be unintentionally collected (collateral intrusion). All data collected will be treated with sensitivity and consideration of impact on individuals. Processing will be kept to a minimum, necessary and proportionate to the legitimate interest.

Is it data which people are likely to consider particularly 'private'?
People may consider some data captured with the use of BWC particularly 'private'. The Standard Operating Procedure will direct staff on how to manage particularly 'private' situations when there is a legitimate interest to activate the BWC. This may be the case when a patient is in a state of incomplete dress or attending to personal care matters.

Are you processing children's data or data relating to other vulnerable people?
It is not anticipated that there will be processing of data relating to children. By virtue of being an inpatient within the ED setting there is an aspect of vulnerability to all patients who will be the data subjects.

Is the data about people in their personal or professional capacity?
The data will capture staff in their professional capacity. If the staff member activated their camera there will be audio recording of their interactions. Data capture of patients will be within the context of ED setting.

Reasonable expectations

Do you have an existing relationship with the individual?
Not always. Given the setting being ED many individuals in the vicinity will be new to the setting and staff present. However, there is a possibility of re-attenders who are familiar with ED staff and have an existing patient-to-professional type relationship.

What's the nature of the relationship and how have you used data in the past?
The relationship will be on the basis of nurse/professional context. Other forms of data is collected and processed in relation to data subjects. Information posters and privacy notice will be available online and to patients and their relatives on arrival. Information relating to the capture of data and processing will be made available throughout the duration of individual's time in ED. Data regarding violence and aggression incidents is already captured within the Trust Risk Management System (DATIX) and considered by the MOVA T&F Group which reports to the Trust Health & Safety Committee.

Did you collect the data directly from the individual? What did you tell them at the time?
The Engagement Advisory Board (Service User Representative Forum) has been involved in the planning of this BWC initiative. Their views have helped shape the content of the poster and FAQ/Information Booklet to accompany the pilot.

If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
Data will not be obtained from a third party as part of this pilot.

How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
No data has been collected as yet.

Is your intended purpose and method widely understood?
We believe so. The intervention is not a first within the NI region and is widely adopted in England and in many other jurisdictions. The intended purpose and method is understood by staff and the patient group and a detailed SOP and policy will be published online as part of the Public Consultation to help inform those wishing to understand the intervention and provide feedback on both intervention and accompanying documents. To-date as part of phase 1 planning there has been wide pre-consultation engagement with key internal and external stakeholders and as part of this the Sub-group coordinating the pilot have educated staff on the legitimate aims, proposed approach and addressed any initial concerns or queries raised. There is a Standard Operating Procedure to support staff's awareness of the purpose and method of use of the body worn cameras.

Are you intending to do anything new or innovative?
As above, the intended intervention while still innovative is not the first adoption within the region or UK. There is a growing body of evidence and research on the use of the devices and these devices have been adopted by many other industries including security, retail, hospitality, police etc. More, it is common place for video phones and recording devices to be operational within public settings by members of the public and this in turn should desensitise the newness and possible sensitivity of the intervention. Nonetheless, through Consultation we hope to engage with our stakeholders and listen and respond appropriately to their views prior to making a decision to continue.

Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation?
Yes, as set out within the stakeholder engagement aspect of the DPIA (Step 7), the Trust has engaged and networked with a wide number of internal and external stakeholders as part of pre-consultation preparation.

REF: Related Research/Articles/Best Practice Guidance

Articles - EDs in England using BWCs.zip

Journals BWC.zip

Best Practice Guidance.zip

Are there any other factors in the particular circumstances that mean they would or would not expect the processing?
None identified at this time

Likely impact

What are the possible impacts of the processing on people?
The evidence base for the use of this technology has strongly indicated such recording has the impact of leading to a change in behaviours in individuals who have the capacity to be aware of their behaviour. It provides additional safeguards for those lacking capacity as it provides a transparent account of the incident. These additional safeguards can also be utilised when there is a complaint of any nature, a safeguarding matter or any matter subject to an investigative process. It is hoped the initiative will have a positive impact on psychological safety of both patients and staff.

Will individuals lose any control over the use of their personal data?
While data subjects will be entitled to their personal data they can make an application for this via the Data Controller as per existing processes and this will be detailed in the bespoke Privacy Notice for the pilot. Individuals will not be entitled to third party personal data, especially if disclosure of such data could cause harm. Therefore, data will be appropriately managed in accordance with UK-GDPR and the category of information considered when dealing with subject access requests (SARs). Third-party requests for data will be considered on a case-by-case basis. The built in redaction tool within the accompanying BWC device software (DEMs-360) will enable the redaction of third party data captured and lessen any potential impact.

What is the likelihood and severity of any potential impact?
It is acknowledged that use of BWC devices may raise some concerns around processing given that recording will take place in an area that patients would not normally expect, the vulnerability of the data subject (patient) and it is recognised that BWC devices have capability of processing background secondary and third party information. In so far as is practicable, and in an attempt to minimise collateral intrusion on those not directly involved, staff using BWC devices will be trained to restrict recording to areas and persons necessary in order to obtain evidence relating to an adverse event. This will be addressed within the aligned SOP and training. For incidents/events which result in criminal activity, the data captured could be requested as part of an investigation as police evidence. The Trust will be required to comply with any internal or police investigation.

Are some people likely to object to the processing or find it intrusive?
Some individuals may object to the capture and processing of data due to personal choice, awareness of inappropriateness of actions and potential implications of these, mental illness especially if the individual is paranoid. They may find it intrusive and in acknowledging this the Trust will be offering information on the aim to be achieved, purpose and restrictions of processing and support to the individual. A protocol for management of this has been built into the accompanying SOP, notably - Use of BWC devices has been introduced for legitimate purposes (lawful basis). Any objection by a service user or member of the public to the use of BWC devices to record, must be addressed by the BWC Operator/IR, when it is possible and safe to do so, with a clear and concise explanation why recording is taking place. This should make reference to the benefits of recording the encounter, which may take account of the recording being a safeguard for all parties by ensuring an accurate reflection of any action or comments made by either party. Reference should also be made to the signage and privacy notice (Digitally available via scanning QR code on signage, available on Trust website and hard copy available at ED Reception). Consideration will also be given to vulnerable person (due to illnesses and mental capacity) encounters and where possible, such individuals should be reassured. 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 BWC Operator/Initial Responder (IR) to make a judgement based on the facts and view at that time and where able the BWC Operator/IR should state the intention to stop recording together with a brief explanation before de-activating their BWC device. Additionally, if at any time the BWC Operator/IR considers it inappropriate to continue to record specific events the BWC Operator/IR can take the decision to end recording and in doing so explain verbally before the recording is stopped. The BWC Operator/IR must then also record the rationale for the decision in the accompanying BWC Recording Event Log and Datix report.

Would you be happy to explain the processing to individuals?
The Trust will be open and transparent in relation to information available to individuals on the processing of data. Staff in the ED areas involved with piloting will receive training and information on the use of BWC and the processing of data. There is a coproduced information leaflet available to patients and carers and easy to read coproduced posters to

provide appropriate explanation to individuals. A Privacy Notice will be available for additional information and who to contact to make a request for personal data.

Can you adopt any safeguards to minimise the impact?
Safeguards to minimise the risk will be:

- Processing as per the principles of necessity and proportionality and based on assessment of risk;
- Staff wearing BWC devices cannot copy or edit any images – this is reserved to senior management with access to the associated video management software;
- Software access will be limited and use will be audible;
- Policy and procedure will be in place for the use and management of BWC devices;
- All staff involved will receive appropriate training, with consideration of managing impact on those recorded and inclusion of policy safeguards;
- Appropriate notices, information leaflets and verbal information to individuals;
- Disposal of data as per retention schedule within DPIA and GMGR 2017;
- Redaction of third party visual images, where necessary.

Can individuals Opt-out?	No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interest's basis.

Can you rely on legitimate interests for this processing?	Yes
Do you have any comments to justify your answer? (optional) The complexity of the initiative and the data to be processed has been considered within a Data Protection Impact Assessment and is supported by governing documents. All of which, speak to the Trust's considerations of UK-GDPR 2018, the impact on individuals and safeguards put in place for the pilot.	
LIA completed by	Edward M. Smyth, Divisional Governance Lead Medicine & Emergency Medicine and Member of the BWC Sub-Group.
Date	10/01/2025

What's next?

Keep a record of this LIA, and keep it under review.

This document will be held with the pilot BWC project documents and will be reviewed again following the evaluation stage of the pilot.

Do a DPIA if necessary.

DPIA completed and also available on Trust website as part of the consultation.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.

This has been completed. A copy of the LIA and privacy notice will be made available as part of the consultation document bundle.