HSC Data Protection Impact Assessment (DPIA) Template

What is a DPIA?

A DPIA is an assessment of the personal data used for a new, or a change to, a system or service. The assessment involves completing a document called a DPIA template. Through this process, risks and measures to mitigate those risks will be assessed. The DPIA is therefore an important document in demonstrating due diligence in terms of data privacy and security; however, it is not the formal agreement to share information or to proceed with a project or system.

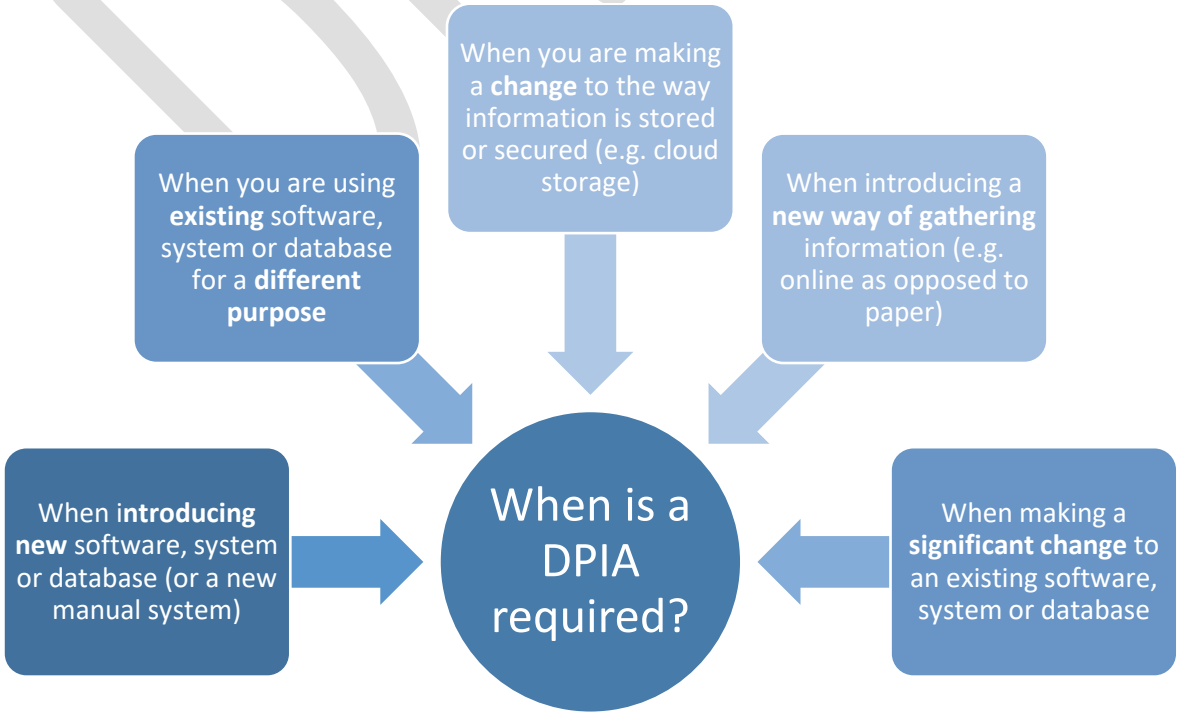
A DPIA forms part of the 'privacy by design' approach to the handling of personal information and allows services to demonstrate compliance with data protection legislation.

WHY DO A DPIA?

It is mandatory for services to complete a DPIA when introducing any new or a change to a system or service that will involve the processing of personal data.

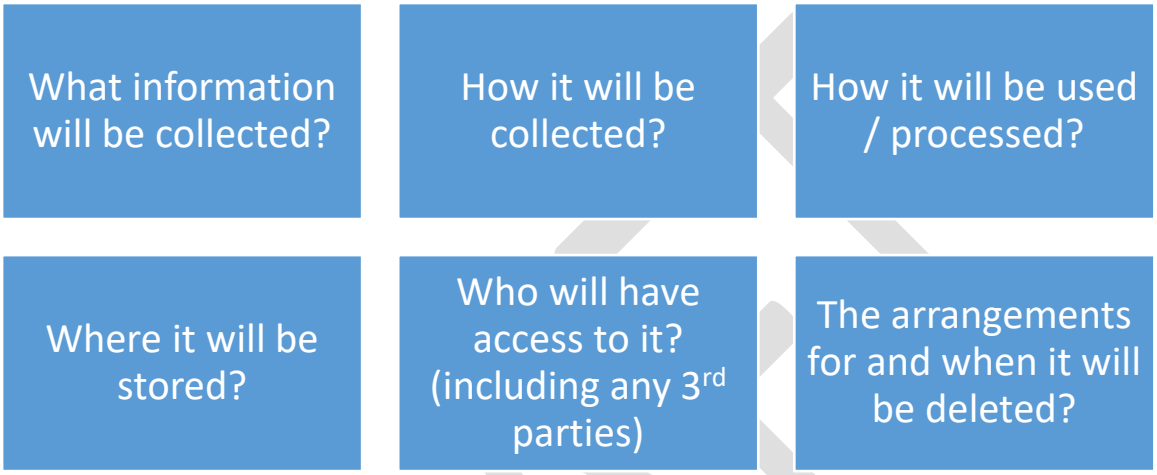
When is a DPIA required?

Data Protection applies to any process involving personal data about living individuals.



The purpose of a DPIA

Completing a DPIA will allow you to identify any privacy risks with your new system and help you to put the necessary safeguards in place to mitigate those risks. An assessment of privacy risks is only possible if you fully understand how personal data will be used. Charting the information or developing a **data flow map** is therefore a key part of the DPIA process so you must clearly describe or explain:



The data protection or privacy risks associated with a project will be closely linked to the data protection principles as set out in UK GDPR (see Appendix 3 for examples of risks).

When should you complete a DPIA?

It is important to begin completion of the DPIA at the outset of the process to avoid delays at a later stage.

Who is responsible for completing a DPIA?

Responsibility for completion of DPIAs lies with the Service Lead or Project Lead that is introducing the new system/process, responsible for that service/business area. The Service Lead or Project Lead will complete the DPIA based on their knowledge of data flows, information systems and related risks. The Information Asset Owner/IAO (a senior Manager or the Assistant Director responsible for the service area) is responsible for ensuring a DPIA is completed by the Service Lead, should be kept appraised and will provide final sign-off. The IAO will ensure that no data processing will take place until this DPIA has been completed and signed. The IAO will also ensure that this DPIA is reviewed and updated if the data processing changes.

Who should be consulted?

Consultation is an important part of the DPIA process and should be built into all stages of the process. This may involve seeking the view from internal or external sources who can provide advice based on their area of interest or expertise (e.g. IT/ICT/Digital Services Department, Information Governance (IG) staff or external providers); or those who will be affected by the new project (e.g. staff or service users). IT/ICT/Digital Services Department approval is a separate process which sits alongside the DPIA. A DPIA focuses mainly on the data protection issues of a project or initiative. The DPIA should focus on the risks to the privacy of the data subjects.

What other documentation might be required?

The main purpose of a DPIA is to assess the data protection aspects of a new system or service. It will document the identified risks and measures that will be taken to mitigate those risks.

A DPIA is considered a "live" document and should be updated when changes to the processing occur. Conducting a DPIA is part of a wider process, e.g. procurement and as such separate documentation may also be required to support the DPIA and give context to the scope of the personal data processing, such as a Business Case, a Data Sharing Agreement or a Contract (which can be referred to within your DPIA).

What is the sign-off process for a completed DPIA?

The sign-off process for all DPIAs is:

1. Draft DPIA is completed and shared with IG Dept (and IT/ICT/Digital Services Department if applicable). Once agreed by all parties the draft version is signed off by the Project or Service Lead;
2. IG will then send it to the Data Protection Officer (DPO) to consider data protection compliance issues and advise on whether the data protection risks are identified and mitigated appropriately DPO will sign off once reviewed.
3. The DPIA is returned to Service/Project Lead to Share with their Information Asset Owner (IAO) for their consideration and approval. The IAO is required to sign off on any residual risks that cannot be mitigated. Once signed off by the project lead, DPO and IAO a copy should be returned to the IG department for logging.

Data Protection Impact Assessment (DPIA) template

The DPIA outlines

- what personal data will be processed?
- what will the information be used for?
- any risks associated with the processing.
- steps taken to mitigate against the risks.

Project/System name: Proposal to Pilot Body Worn Cameras in Emergency Departments at RVH & MIH sites for 6 months
Service or Project Lead – completing the DPIA **Name: Colin McMullan / Linsey Sheerin** **Telephone: 02896 156130** **Email Address: colin.mcmullan@belfasttrust.hscni.net / linsey.sheerin@belfasttrust.hscni.net**
Department/Location (include full address) Emergency Departments @ Royal Victoria Hospital & Mater Infirmorum Hospital
Directorate: Unscheduled Care
Date DPIA commenced: TBC
Version number: 20/11/25

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**

As part of this first stage, the service area may need to complete a Data Flow Map. This can be a diagram but should accurately describe the stages of the data flow from beginning to end.

Context
Emergency Departments across the Belfast Health and Social Care Trust (BHSCT) — including the Royal Victoria Hospital (RVH) and Mater Infirm Hospital — face sustained and escalating levels of violence, aggression, and abuse towards staff.

These incidents occur against a backdrop of overcrowding, long waits for assessment and admission, and high levels of alcohol and substance-related presentations.

Scale of the Problem

- The RVH ED, as the regional major trauma and tertiary centre, records the highest number of violent and aggressive incidents within the Trust.
- Data from Datix and incident logs show a persistent pattern of verbal abuse, threats, and physical assaults, often directed at triage, nursing, and security staff.
- Under-reporting remains a recognised issue — many staff report that abuse has become “normalised” within daily work.
- The problem extends beyond physical harm, encompassing psychological trauma, burnout, and moral injury among frontline teams.

What information will be collected

BWCs will be used by staff, following training, to record footage (video and audio) in specific circumstances and only after other strategies to de-escalate a situation have been exhausted (in line with Belfast Trusts Zero Tolerance and the regional Management of Violence and Aggression framework). Staff will be advised, that BWCs may be activated and reasonable to use when there is a threat of violence and aggression or actual violence and aggression against staff and others in their clinical area. Staff will be advised not to record anything that risks adversely impacting the safety, dignity and/or on-going care of any person. BWCs will not be used in situations where personal care and intimate treatment/care, or intervention is occurring.

How it will be collected
BWCs store digital files which, once recorded cannot be viewed, deleted or amended by the operator or any other member of staff except for those designated persons noted in the Standing Operating Procedures (SOPs).

BWC Device & Upload / Transfer of Information:
All BWC devices must be returned to a docking station immediately after operational use. Docking the camera will result in the recorded footage being automatically deleted from the camera and downloaded to the secure server.

All recordings/data will be automatically deleted from the secure server after 28 days unless an incident is raised via the online DATIX system.

How recordings will be used / processed
Disclosure of information from any of the Trusts BWCs will be controlled and consistent with reference to the purpose(s) for which the scheme was established.

The date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) will be recorded accordingly. Each recording will be viewed and, if necessary, images of persons not directly involved in the incident will be obscured to protect their identity and comply with data protection requirements.

When disclosing images of individuals, consideration will be given to whether or not obscuring of identifying features is necessary. Whether or not it is necessary to obscure will depend on the nature and context of the footage that is being considered for disclosure.

Judgements about disclosure should be made in conjunction with the Trust Information Governance Team. The team have discretion to make an assessment regarding disclosure within the context Data Protection Legislation.

Once the information has been sent to another body, such as the police, they then become the data controller for the copy they hold. It is their responsibility to comply with the Data Protection Act (DPA) and UK GDPR in relation to any further disclosures.

The method of disclosing information will be secure to ensure the footage is only seen by the intended recipient/s.

Where it will be stored
All recorded footage will be held on the secure server for 28 days before being automatically deleted. Recorded footage which is required beyond the 28 days for evidential purposes must be marked as an incident. A DATIX (Trust internal management of information system) detailing the incident must be completed to retain the footage beyond the 28 day period.

Who will have access to it (including any 3rd parties)
The information will be encrypted and cannot be accessed by the BWC device user. Details of the incident must then be recorded on DATIX referencing the BWC device serial number and docking station serial number.

The arrangements for and when it will be deleted
All recorded footage will be held on the secure server for 28 days before being automatically deleted.

If your processing includes the use of emerging technologies e.g. **Artificial Intelligence (AI)** then this needs to be specified in more detail below:
Please see the ICO's guidance on AI AI and data protection risk toolkit | ICO

STEP 2. ASSESS THE NEED FOR A DPIA				
Screening Questions- The following are intended to help decide whether a full DPIA is necessary.				
Number	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 information in a new way?	☒	☐	BWC devices are a new technology which are not currently used in BHSCT but are being currently piloted in Northern Trust ED setting. Considering that these devices will be worn by Security Officers assigned to ED and Nursing Staff, there is the potential for more data to be obtained than

				by the current static CCTV system in situ.
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 BHSCT 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 BHSCT 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 BHSCT. 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 BHSCT is new technology use. There is no existing processing of this nature within the BHSCT or within ED settings across the region. As part of the introduction of BWCs, the

				BHSCT 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 BHSCT 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 BHSCT 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? Or is there a DPIA in place but this is a new instance of processing?	New ☒ Update ☐ *If this is an update to an existing DPIA please provide details*		

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

If you have answered <u>NO</u> to all of the 8 questions above <u>please proceed to Step 12 and record the outcome</u>.

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	☐	
Telephone/mobile number	☐	
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	☒	Personal images of staff, services users, relatives and visitors could all potentially be captured on BWC
Other* please specify all other personal data	☒	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 (a) recordings will take place in an area that patients would not normally expect and (b) the recordings may involve potentially vulnerable people (data subjects). However, the use of public consultation to support the development of policy and supporting documentation will help minimise 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 limited 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. Covert recording will not take place and those in the proximity will be notified where practically possible before devices are activated, promoting transparency.

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 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	☒	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.
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	☒	Possible that cultural dress captured in footage may give an indication to a particular religion

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	☒

*__Relevant to 6, 1 (c) only__, Please provide details of the relevant sections of legislation in addition to UKGDPR, which support your legal basis

N/A

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 will be specified in the BWC Pilot Privacy Notice and Consultation document.

Legitimate interests noted to date include:

- 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.

Belfast Trust 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.

<u>Other Legislative Considerations</u>

- **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 has given consideration to the Surveillance Camera Commissioner 's (SCC) best practice guidance, the 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.

  With regard to the Human Rights Act 1998 Belfast Trust focused on three rights **namely Articles 3, 8 & 14** (on the basis that these are most relevant to the use of BWCs) thus ensuring our approach is lawful, for a legitimate aim and proportionate. By consulting local experts we have also given consideration to Deprivation of Liberty (DoL) and Mental Capacity issues.

  Our proposal is drafted with all these statutory obligations in mind. Our approach is based on the principle of 'a less restrictive option' (re:Art8) by only switching cameras or recording equipment on when an activation criteria is met. Our privacy notice and pilot documents set out our rational for use and our legitimate aims and the safeguards which are an integral aspect of our proposal.

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 an existing diagnosis which has deteriorated. It certainly is not our intention to distress anyone or make individuals feel humiliated or frightened (re Art3). This DPIA and supporting documentation clearly sets 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 our Eds to 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. Moreover, our activation criteria 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**? See Appendix 2 for further information or seek IG advice.

Article	**Lawful Basis**	**Tick**
9 2 (a)	Consent	☐
9 2 (b)	Employment social security social protection law	☐
9 2 (c)	Vital Interests	☒
9 2 (d)	Legitimate interest	☐
9 2 (e)	Already public	☐
9 2 (f)	Establishment, exercise or defence of Legal claims or judicial capacity	☐
9 2 (g)	Public Interest	☐
9 2 (h)	Health and Social Care treatment or management of HSC systems	☐
9 2 (i)	Public Interest in the area of Public Health, Quality and Safety of Health Care	☒
9 2 (j)	Archiving in the public interest, scientific, historical research or statistical purpose	☐

	Article 9 of UK GDPR allows for processing in relation to Special Category data where it is necessary for {but not limited to) the protection of the vital interest(s) of another natural person; or for reasons of substantial public interest as detailed in Schedule 1 part 2 of Data Protection Act (2018) which includes but is not limited to, 'preventing or detecting unlawful acts' and 'safeguarding children and of individuals at risk'. Pursuant, Article 10 of UK GDPR allows the processing of personal data relating to criminal convictions and offences. BHSCT fully understands that the utilisation of BWC must be lawful and fair. All processing of personal data which does fall under the remit of the UK GDPR must be fair and lawful. This means we must have an appropriate legal basis or justification, for using BWC as required by Article 6, 9 and 10 of the UK GDPR and as outlined above.	

STEP 5: ASSESS SECURITY OF THE INFORMATION

Will the information be shared with, hosted by or transferred to another organisation or third party? YES

If NO – move to Step 6

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.

Other 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 by Trust ICT, through use of portals etc.

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.

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	X	☒
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)	☐	☐

How will you secure the information in Transit? Tick which apply	
Encrypted Email	☐
Shared internally over secure network	☐
Secure file transfer	☒ for SAR's/Third Party Requests may be shared via secure file transfers
Secure Cloud Server	☒AES 256 Cloud Hosted solution by supplier, reveal media Ltd.
Amazon AWS or Microsoft Azure	☒ AES 256 bit in Microsoft Azure
Registered post via post safe envelopes / secure post service	☐

ICT Input			
Have you sought approval from your IT/ICT/Digital Services Department? **If you have answered NO or N/A, state your reason and proceed to step 6**. If **YES** continue to answer the remaining questions in this section	YES ☒	NO ☐	N/A ☐

Has a 3rd party technical questionnaire/Cyber Security questionnaire been completed and approved by IT/ICT/Digital Services Department?	YES ☒	NO ☐	N/A ☐
If the cloud storage platform is not Amazon AWS or Microsoft Azure, please answer the following questions: Has the solution been PEN tested? (Penetration Tested – Please provide a copy) Does the solution have Anti-Virus software? Does the solution have Anti-Ransomware? Is multi factor authentication available?	YES ☐ YES ☐ YES ☐ YES ☐ YES ☐	NO ☐ NO ☐ NO ☐ NO ☐ NO ☐	N/A ☒

STEP 7. CONSULTATION PROCESS

You should consider the impact of the new process or system will have on all your stakeholders. Who have you consulted with?

An extensive programme of engagement with key stakeholders to help develop our proposal was undertaken between April 2025 and August 2025. This involved discussions with the following groups of people:

Staff X
Service Users☐X
IG Department X
IT Department X
Internal/external Partners (please list) X
Statutory agencies (please list) X

A detailed and comprehensive engagement report is attached.

If you have not consulted with affected staff or service users please explain your reason for this below: N/A

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? If **No**, please ensure the risk of function creep is included at **Step 1**	YES ☒	NO ☐

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 void 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 BHSCT 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 BHSCT 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 BHSCT 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 Consultation Document, a FAQ and an EQIA. Following consultation, all feedback will be considered with a view to amend and improve the documentation, as necessary.

There will be two levels of staff training – BWC Operator/IR and Administrator/Nurse 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/ 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/ Nurse 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.

BWC devices and associated software will be registered information assets and managed by the Information Asset Owners (IAOs), which involves definition purpose, 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. Information will only be captured and processed to achieve a legitimate aim, as detailed.

At all stages, the BHSCT will comply with the UK-GDPR and the Data Protection Act and other legislation such as Equality, Good Relations and Human Rights legislation.

Specifically, in relation to the Human Rights Act there will be adherence to the requirements of Article 6 (Right to a fair trial), Article 8 (Right to respect for private and family life, home and correspondence) Article 3 (Right not to e tortured or treated in an inhuman or degrading manner and Article 14 (Right not to be discriminated against).

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
- 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

- The Roles and Responsibilities of Trust staff will be set out clearly as part of the BWC 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 BHSCT DEMS-360 installation. This prevents any access to the footage outside of BHSCT DEMS-360 software.

- Specific PCs in proximity to the Office where the BWC are located 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. Once uploaded, the footage is automatically deleted from the device.

- Access to the DEMS-360 software is username and password protected and only Administrators with the designated permissions can turn off "Encryption" and "Trusted Mode" 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 ICO's 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 a policy, SOP, FAQ, Privacy Notices, bespoke training and existing processes and controls adopted by Belfast Trust to maintain the quality and accuracy of data processed on servers

The associated BWC Policy can be read in conjunction with a number of supporting Trust policies and will be aligned to the necessary legislative obligations including but not limited to:

- UK-GDPR
- Data Protection Act 2018
- ICO Guidance on Video Surveillance (including CCTV)
- Surveillance Camera Code of Practice
- Regulation of Investigatory Powers Act 2000
- DoH Good Management, Good Records 2017
- Management of Violence & Aggression Framework 2022
- Implementation of the Mental Capacity Act (NI) 2016
- Deprivation of Liberty Safeguards 2019.

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 will 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 ICO's 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? *(If no, a bespoke privacy notice will be required and approval sought through IG Department)* 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, DPO and ICO, the purpose and lawful basis for processing data as well as retention schedule and individuals rights. 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.	YES ☐	NO ☒
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 ☒	NO ☐

STEP 10. PERSONAL INFORMATION SHARING AGREEMENTS		
Is there or will there be a **contract** 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*	YES ☒	NO ☐

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:

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.

To assist you in identifying potential or likely privacy risks you will find a non-exhaustive list of possible risks at Appendix 3.

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 Include <u>associated</u> compliance as necessary *(See Appendix 3 for examples). Please separate your risks out on separate rows*	**Likelihood of occurrence** 1. **Rare** - This will probably never happen/recur 2. **Unlikely** - Do not expect it to happen/recur but it may do so 3. **Possible** - Might happen or recur occasionally 4. **Likely** - Will probably happen/recur, but it is not a persisting issue/circumstances 5. **Almost Certain** - Will undoubtedly happen/recur on a frequent basis **Refer to HSC Risk Matrix above** **ENTER NUMBERS BELOW**	**Severity of harm (if occurred)** 1. Insignificant 2. Minor 3. Moderate 4. Major 5. Catastrophic	**Overall Risk** **(use Matrix, to calculate overall risk)** Low Medium High	**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 Or Accepted* **(*Select 'Accepted' where 'Overall risk' is rated as 'Low')**	**Residual risk** Low Medium High
Equipment failure/ Malfunction and Loss of Footage	3	2	Medium	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	Choose an item.	Choose an item.

				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 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	3	2	Medium	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 will be monitored by local	Choose an item.	Choose an item.

				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. [Need to check if data can be remotely scrubbed] 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	3	3	High	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	Choose an item.	Choose an item.

				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. 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)	3	3	High	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	Choose an item.	Choose an item.

				managers associated with the ward area/division management. Use of the software can be reviewed through a system created audit trail.		
Server failure due to fire, flood, viruses, other.	3	4	High	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, provided servers remain intact or located in another setting (in context of fire/flood	Choose an item.	Choose an item.
Function creep resulting in non-compliance with legislation and bringing potential for fines	3	3	High	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.	Choose an item.	Choose an item.

				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 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.	Choose an item.	Choose an item.
Increased costs associated with the use of equipment, management of software	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

impacting on service budget.						
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 12-14 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.	Choose an item.	Choose an item.
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 responses/legislative compliance regarding the same.	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 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.		
Proximity and vantage point of BWC cameras may increase level of privacy intrusion and potential to capture footage showing 3rd parties and individuals in distressed state.	3	2	2	The wide-angle vantage point of the BWC cameras is something acknowledged within the BWC. Privacy notices and posters will be on display within the ED to alert members of the 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	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		
	Choose an item.	Choose an item.	Choose an item.			

Add additional rows as required.

*** As per Step 10 please ensure the contract or relevant sharing agreement contains data protection clauses and covers the risks identified above**

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:	
Name and Job Title:	
Signature:	**Date:**

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

Summary of DPO advice:	
Name:	
Signature:	**Date**:

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:	
Signature:	**Date**:

Please return a copy of the final signed DPIA to the Information Governance Department

Appendix 1 - Data Protection Principles

The data protection principles are contained in the UK GDPR and require that personal information must be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject - (Lawfulness, Fairness and transparency). There must be valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data and you must not do anything with the data in breach of any other laws. Personal data must be processed in a way that is fair and not unduly detrimental, unexpected or misleading to the individuals concerned. You must be clear, open and honest with people from the start about how you will use their personal data.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (Purpose limitation)

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - (data minimisation)

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Storage Limitation)

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)

In accordance with Article 5(2) of the UK GDPR the data controller shall be responsible for, and through its policies, procedures and protocols will demonstrate compliance with the Data Protection Principles listed above **(overarching principle of Accountability).**

Appendix 2 – Lawful Basis for processing Personal Information and Special Category Information

You must have a valid lawful basis in order to process personal data in compliance with Article 6 of UK GDPR.

If you are processing special category data*, you also need to identify a further special category condition in compliance with Article 9 of UK GDPR.

You should document your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability

The lawful bases for processing are set out in **Article 6 of the UK GDPR**. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. *(NB. Please consult with your IG Department before using this as your lawful basis for processing personal data. This cannot be applied by a public authority processing data to perform its official / core function (e.g. processing data as part of the provision of health or social care) however may be relevant for non-core functions such as HR)*

Special category data is personal data that needs more protection as it is more sensitive than basic personal data. The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;

- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Article 9 lists the conditions for processing <u>special category data</u>:

(a) Explicit consent

(b) Employment, social security and social protection (if authorised by law)

(c) Vital interests

(d) Not-for-profit bodies

(e) Made public by the data subject

(f) Legal claims or judicial acts

(g) Reasons of substantial public interest (with a basis in law)

(h) Health or social care (with a basis in law)

(i) Public health (with a basis in law)

(j) Archiving, research and statistics (with a basis in law)

See the Information Commissioner's Office (ICO) website (links below):

- For more detail on each lawful basis for processing personal data

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

- For more detail on the additional conditions for processing special category (sensitive) personal data

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Appendix 3 - Examples of possible risks include: Please note that not all these risks are applicable to every project, nor is this list exhaustive. Please ensure that the risks you list in step 6 are relevant to your project.

DP Principle (see App 1)	*Example Risk*	*Example Mitigation*
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	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	• 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 • 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 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 adhoc 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.		