North East Ambulance Service NHS
NHS Foundation Trust

North East Ambulance Service neasus Unified Solutions

Data Privacy Impact Assessment

Document Control Sheet

Q Pulse Reference Number	SOP-F-IG-5
Version Number	02
Document Author	Information Governance Manager
Head of Department/Executive Director Job Title	Director of Finance & Resources
Head of Department signature	
Date Approved	17 July 2018
Date form Effective From	17 July 2018
Next Review Date	17 July 2021
Keywords	Data controller; data processor; data protection; DPIA; information asset owner; governance; privacy; risk assessment; system.
Target Audience	Senior Managers, Information Asset Owners

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

Introduction

This DPIA template is based on the Information Commissioner's Office (ICO) template of how you can record your DPIA process and outcome. It follows the process set out in the ICO DPIA guidance, and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

1. Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Body Worn Video – Operations staff The North East Ambulance Service (NEAS) Operational Directorate wishes to undertake a trial of cameras that are capable of capturing both video and audio information and are known as Body Worn Video (BWV). These will be used by uniformed Operational staff and be fitted to their clothing. With the progression of technology, the devices have become smaller, lighter, and more easily carried by staff. It is widely known that members of the public, going about their daily lives, are likely to have their movements and identity captured on a multitude of surveillance systems and it is of paramount importance to mitigate any privacy risks and issues associated with BWV. There is a requirement to undertake a DPIA due to the implementation of new technology which processes special category personal data. **Objectives of using BWV:** • To protect staff, patients and members of the public. • To protect NEAS assets. • To increase personal safety and reduce fear of crime. • To reduce incidents of violence and aggression to staff members. • To support the Police in reducing and detecting crime. • To assist in identifying, apprehending and prosecuting offenders. • To provide a deterrent effect on violence and aggression towards staff. The Trust will review this DPIA in light of ongoing consultation with its community, in response to any national and legislative changes and best practice guidance from the relevant organisations.

2. Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Collection:
Body Worn Video (BVW) equipment consists of a small camera attached to the uniform of Operations staff which record visual and sound data. The purpose of the recording is to safeguard staff, patients and the public during violent and aggressive or anti-social behavior incidents. The footage will be in an encrypted format, securely stored and only viewed by authorised persons.

Use:
The devices will only be activated during an incident and continuous recording is strictly not permitted.

Store and deletion:
Visual and sound recordings will reside on the device until it is 'docked'. Once docked, the RFID card must be used to access the recording and enable it to be sent to the server. The will remove the recording from the device. Once the recording is on the server, it will automatically be deleted after 30 days unless transferred from the server.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

As part of the 3 month trial, 12 devices will be provided. They will be deployed in various location across the Trust. The devices will only be switched on for recording audio and visual when the staff member believes an individual is being aggressive or there is the potential for aggression.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The Operations staff will make the decision on a case by case basis whether to switch on the device to record. The individual(s) on scene will be shown the device and informed verbally that recording is in progress – there will be no covert recording. The BWV SOP details what should be done if people object to be recorded or if they ask for an event to be recorded and when they should stop recording. Equally, staff may have to justify not recording in any particular circumstance.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
• Deterrent and encourages compliance through self-awareness. • Supports de-escalation of violence. • Safety of staff by reducing verbal and physical attacks. • Contribute to the transparency of security procedures. • Provision of verifiable recordings with time-stamp & support statements. • Saving lengthy descriptive reports having to be provided. • Footage is readily acceptable by courts and CPS. • Acceleration of judicial process by encouraging early guilty pleas. • A reduction in complaints against staff. • BWV should reduce absenteeism by supporting with all the above. • A tangible contribution to efficient work flow and cost savings.

3. Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
The following stakeholders have been consulted: • NEAS IM&T Department • Quality Governance Group (chaired by Caldicott Guardian) • Health and Safety Committee • NEAS Operational staff • NEAS service users (Patient, visitors, relatives) • Staff side organisations • North East NHS Trusts/CCGs • Northumbria Police Force • NHS England • NHS Improvement • Welsh Ambulance Service The Trust will advertise their proposal to use BWV by means of a notice in the press, online on the Trust website and via social media. We have consulted with many staff and groups as identified in section 3. This had entailed a demonstration of the system and feedback on its use. The team are working with Ward Hadaway to finalise the Surveillance Camera Policy. The Trust will continue to publicise the use of this equipment to ensure that the public are fully informed of their use.

4. Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The Trust has established the need for the use of cameras that are capable of capturing both moving images and audio information which are worn by uniformed Operational staff for the purposes described in section 2. Further use of BWV will require separate DPIAs to be carried out.

Operational staff will only deploy BWV technology against the defined operational requirements (where there is risk of violence, aggression or assault potential criminal acts against staff and or the Trust) and ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing staff and patient safety need described in the Trust Surveillance Camera Policy, the assignment instructions and NHS England and NHS improvement advice and guidance.

At all stages it will comply with the Data Protection Act, Health & Safety at Work Act (Duty of Care) and PACE legislation. In the case of the Human Rights Act 1998, 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 earlier. It is important to note that in principle there is no requirement to obtain the express consent of the person or persons being filmed since the actions of the Operations staff are deemed to be lawful.

Previous versions of the Trust CCTV policy have included the procedures and processes for data collection and have been subject of full consultation and approval by Trust Board. The CCTV policy has been recently revised to include BWV and renamed to Surveillance Camera Policy.

Prior to any activation subjects and persons in the immediate vicinity will be informed of the activation by the Operations staff. Immediately on the unit being turned on they will again be informed of its activation. Any non-evidential material is retained for 30 days. This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law. Recorded material is Trust information and it can be accessed on request in writing in accordance with the Data Protection Act, unless an exemption applies in the circumstances.

The BWV operator will decide on a case-by-case basis when and when not to switch the BWV on or off. There should always be a presumption to record if the ‘need to address a pressing staff/patient safety need’ has been achieved unless the circumstances dictate otherwise. Based on the above, the following categories of

members of the public are likely to have their contact recorded:

- Witnesses of lawful activities.
- Witnesses of crimes, or those who witness other parties verbally or physically abusing Trust staff as they discharge their duties.
- Persons suspected of committing offences.

In addition, persons, unrelated to any specific interaction between Trust staff and any of the categories of persons above, might find their activities captured on a BWV device. To some degree, this is inevitable since a camera lens or microphone is non-discriminatory and captures whatever is within its vicinity. The will adopt a number of safeguards to firstly avoid this occurrence where possible and to ensure that the data is held securely until it is no longer required.

As previously mentioned, BWV is capable of capturing primary evidence in such a way that it is able to bring a compelling and an indisputable account of an incident. It will considerably reduce ambiguity. It will not replace the need to capture other types of evidence but should be considered as an additional tool.

BWV will not be routinely recording and monitoring all activity, the always on approach. To do so would fundamentally breach the privacy of large numbers of members of the public, who are going about their private business, as well as to a degree the privacy of Trust staff going about their work. This cannot be justified from the perspective of proportionality and legitimacy.

Added to this, is that current technology is incapable of operating in such a way principally due to a lack of suitable and sustainable battery life. In addition, such a practice would require the storing, reviewing and then disposal of large quantities of data.

In every case where the BWV is activated, the staff member involved must be prepared to justify its use.

All images from BWV have the potential for use in court proceedings whether they provide information that is beneficial to the prosecution or defence. The information will be safeguarded by an audit trail in the same way as other evidence that is retained for court.

It must be emphasised that BWV can collect valuable evidence for use in criminal prosecutions, ensure the Trust acts with integrity and transparency and potentially provides objective evidence of controversial events. It offers protection for both citizens and the Trust. However this justification may be closely scrutinised by a court and it is essential that BWV recordings will not retained where there is no clear evidence of an offence, unless some other good reason exists for their retention.

5. Identify and assess the risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
1. Inappropriate or continuous recording on scene.	2	3	6
2. Inability to switch off visual or audio recording.	2	3	6
3. Holding excessive recordings due to inappropriate or continuous recording on scene.	2	3	6
4. Loss/theft of camera.	1	5	5
5. Loss/theft of RFID device.	1	1	1
6. Unauthorised copying of footage to a personal device.	1	5	5
7. Footage may show victims, potential witnesses, suspects or other third parties in a state of distress and/or undress.	3	4	12
8. The proximity and vantage point of cameras may also increase the level of privacy intrusion when recording footage from within someone's home.	3	4	12
9. The camera device is encrypted (at rest) but the recording is not encrypted in transit to the server based application.	1	5	5
10. The recordings held on the NEAS server are not backed up.	2	4	8
11. Individual may object to being recorded.	3	4	12
12. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.	3	4	12
13. Public distrust about how information is used can damage an organisation's reputation.	3	4	12

6. Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
1.	Provide guidance to BWV users on appropriateness of use of the device. Ensure users are trained in appropriate use. Audit appropriateness of device use per user.	Reduced	1x3 = 3	Yes
2.	Provide guidance to BWV users on appropriateness of use of the device. Ensure users are trained in appropriate use. Audit appropriateness of device use per user. In order to ensure all aspects of an incident are captured, this requires the inclusion of audio information in order for this to be complimentary to the video data. Sometimes the camera may not be pointing in the direction of the main incident but the audio will still be captured. This has a significant advantage of protecting all parties to ensure the actions of the Operational staff are totally in accordance with the law. Equally, the presence of only video evidence without the added context that audio, can fail to adequately provide the full context for all parties of an incident or interaction.	Reduced	1x3 = 3	Yes
3.	Review recordings to retain only those recordings required in line with Trust policy. Edit or obscure sections of the recording if they identify individuals who are not the subjects of concern.	Reduced	1x3 = 3	Yes

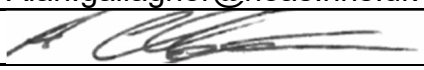
4.	Ensure movement of devices is monitored and they is a checking in/out process. A device may become detach and fall into unauthorised possession with the possibility of the data being accessed by an unauthorised individual. Where a device is lost, all possible attempts will be made to identify and notify persons who are subjects of information on the device. In addition, the captured information is stored on the devices internal memory. To access this requires bespoke docking facility that recognises the device and associated software which is not publically available. Specific software is required form the manufacturer so it is highly unlikely the video can be accessed.	Reduced	1x2 = 2	Yes
5.	Ensure movement of devices is monitored and they is a checking in/out process. Disable the card remotely.	Eliminated	0	Yes
6.	Audit all user of the device and software. Ensure user USB ports are disabled.	Reduced	1x2 = 2	Yes
7.	Edit or obscure sections of the recording if they identify individuals who are not the subjects of concern.	Reduced	1x4 = 4	Yes
8.	Edit or obscure sections of the recording if they identify individuals who are not the subjects of concern. It is inevitable that in some circumstances this will occur and users will be trained to ensure that wherever possible the focus of their activity is on the person subject of the incident. It is widely recognised that citizens are likely to have a strong expectation of privacy in their own homes (article	Reduced	1x4 = 4	Yes

	8 of the Human Rights Act) and under normal circumstance BWV should not be used in private dwellings. However, if when attending for the primary purpose of delivering medical care and a violent and aggressive or anti-social behavior situation arises the BWV may be activated after announcing to the individuals on scene.			
9.	Apply encryption in transit if trial is successful.	Accept	1x5 = 5	Yes
10.	Consider the costs of backing up the server.	Accept	2x4 = 8	Yes
11.	In the event that someone requests that the BWV be switched off, they should be advised that: • Any non-evidential material is retained for 30 days. • This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law. • Recorded information is Trust information and can be accessed on request in writing in accordance with the Data Protection Act unless an exemption applies in the circumstances. Recording can only be justified when it is relevant to the incident and necessary in order to gather evidence of violent and aggressive or anti-social behavior incidents .	Reduced	1x4 = 4	Yes
12.	Ensure the purpose for use of the devices does not change and remains within the legal basis for processing.	Reduced	1x4 = 4	Yes
13.	Ensure full public consultation about the use of the device with the	Reduced	1x4 = 4	Yes

	opportunity to comment.			

7. Sign off and record outcomes

Residual risks approved by:		Comments / recommendations *If accepting any residual high risk, consult the ICO before going ahead.*
Name	Andy Lumsden	.
Email	Andrew.lumsden@neas.nhs.uk	
Signature	*Andy Lumsden*	
Date	04/09/2019	

Measures approved by:		Comments / recommendations
Name	Alan Gallagher	
Email	Alan.gallagher@neas.nhs.uk	
Signature		
Date	04/09/2019	

Information Governance Manager (DPO) approval		Comments / recommendations *DPO should advise on compliance, step 6 measures and whether processing can proceed*
Name	Seema Srihari	It is recommended that this DPIA is circulated to all stakeholders and public for comment prior to proceeding with the trial. The DPIA should then be reviewed to consider the comments.
Email	Seema.srihari@neas.nhs.uk	
Signature		
Date	04/09/2019	

DPO advice accepted/ by:		Comments / recommendations *If overruled, you must explain your reasons*
Name	Andy Lumsden	
Email	Andrew.lumsden@neas.nhs.uk	
Signature	*Andy Lumsden*	
Date	04/09/2019	

This DPIA will kept under review by:		Comments / recommendations
Name	Andy Lumsden	
Email	Andrew.lumsden@neas.nhs.uk	
Signature	*Andy Lumsden*	
Date	04/09/2019	

Appendix A

What are privacy risks?

Privacy risks include the following:

- Risks to individuals or other third parties (for example, misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency).
- Compliance risks e.g. breach of the Data Protection Act (DPA).
- Risks to the organisation (for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public).

A PIA is suitable for:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system.
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring.
- Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed.

Types of privacy risk

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.

- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Compliance risk

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015
- Non-compliance with the DPA.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Associated organisation/corporate risk

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Appendix B: General Operating Procedures

Staff approved to use BWV will 'book out' their BWV device from a pool of devices shared amongst a number of staff. This booking out process, along with their other equipment, is supervised and recorded. This will ensure that a specific device is allocated to a specific member of staff. A specific secure back office BWV computer is used to maintain the integrity and continuity of the device and captured BWV video data. A set of operational guidance notes has been issued complemented by training on the correct use of the BWV device and associated back-office software.

Local managers are required to ensure that the device is charged and all previously captured images and audio is removed prior to redeployment. The device will then be fixed to the staff member's uniform.

During the course of their normal duties, the device remains in a "standby" mode and does not record any material. In order to do so, the staff member must deliberately activate the device and, where practicable, make a verbal announcement to indicate that the BWV equipment has been activated. This announcement should be present on the recording and if possible, should include:

- The nature of the situation to which the user is present; and
- Confirmation to those present that the incident is now being recorded using both video and audio.

If the recording has commenced prior to their arrival at the scene, for example coming to the assistance of another colleague the staff member should, as soon as is practicable, announce to those persons present that recording is taking place and that their actions and words are being recorded. Announcements should be made using plain English that can be easily understood by those present.

At the conclusion of any incident, the record mode on the device is switched off and the captured information is stored.

Unless specific circumstances dictate otherwise, recording must continue uninterrupted from the moment it starts until the conclusion of the incident or the resumption of general patrolling.

The recording is also likely to continue for a short period after the incident to clearly resumed other duties or activities.

Where practicable, users should make an announcement that the recording is about to finish. Prior to concluding recording, the user should make a verbal announcement to indicate the reason for ending the recording. This should state the reason for concluding the recording.

At the end of period of duty, the officer returns the device to their operational base. They must then follow a clearly defined process which involves 'checking in' the BWV device. Their manager, supervisor or team leader 'dock' it into a dedicated port and this automatically downloads all captured information on to the NEAS server. This information cannot be deleted or altered.

Once completed, the contents of the device are erased and it is ready for reuse.

All information captured and downloaded will be retained on the server. Any material required to support potential criminal investigation or prosecution will be retained until passed to the Police via the agreed secure transfer method. The original digital copy of the footage is held until the outcome of any investigation or 2 years whichever is longer.

Data required for complaint resolution or internal investigation will be held securely and retained until completion of the complaint or investigation, or for 12 months whichever is longer.

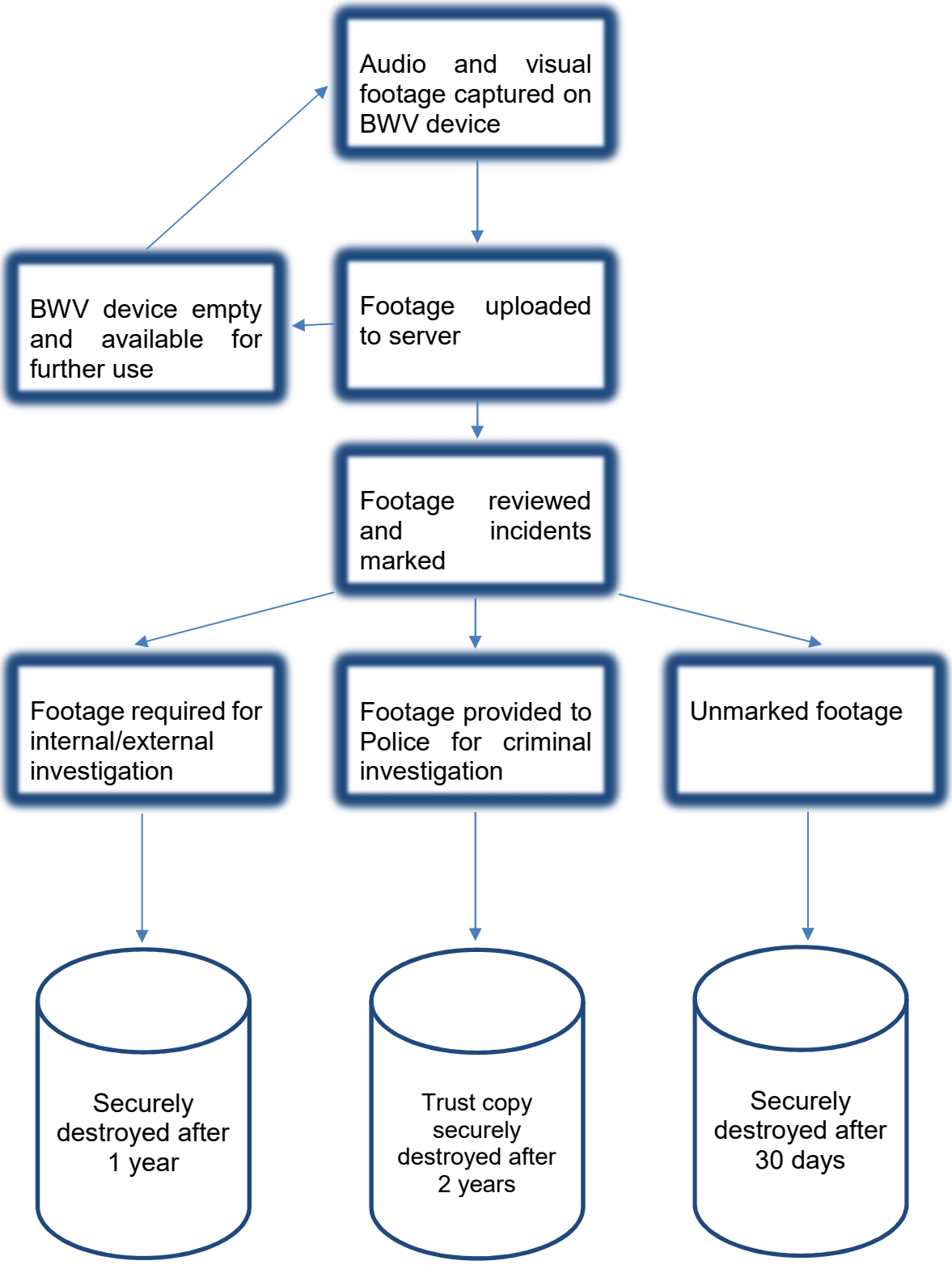
All other material will be automatically erased after 30 days.

Access to retained recordings will be controlled and only persons having an operational need to view specific incidents may do so. The master copy remains as a digital file in the storage device. This is a bit-for-bit copy of the original recording, which is stored securely, pending its production, if required, at court as an exhibit.

A working copy may be produced from the original media (for investigation, briefings, circulation, and preparation of prosecution evidence and defence) by burning on to a DVD.

The Trust will also ensure that data subjects (those whose personal data is captured by the BWV device) are able to access the relevant recordings under the Data Protection Act, unless an exemption applies.

Appendix C: Data Flow



In circumstances where the information is evidential, master and working copies are created and retained. At the conclusion of any investigation / review or complaint, there is a requirement to hold the data in accordance with Trust retention schedules.

Where information is shared with the Police or other body, they will be responsible for the secure retention and destruction of the data in line with their policies.

Appendix D: Frequently asked questions

Through the introduction of body worn video (BWV), there might naturally be concerns associated with how any information is being captured, processed and retained by the Trust. The purpose of this section is to identify what these issues are and to provide an explanation of the mitigation the Trust will apply, to ensure the risks are kept to a minimum.

1. BWV introduces new and additional information technologies that have a substantial potential for privacy intrusion.

BWV is an expanding technology being utilised by the Trust as part of the CCTV Policy. However, the Trust recognises the concerns from the public regarding privacy issues. Accordingly, this technology will only be deployed in an overt manner, using trained uniformed staff and in defined operational circumstances. All captured data will be processed to ensure total compliance with the Data Protection Act and Human Rights Act, and retained and subsequently disposed of in accordance with the Trust's operational guidance.

2. BWV technology allows information to be shared with multiple agencies

When capturing information on these devices, Trust staff will only do so in order to fulfil a legal purpose such as sharing with the police when an offence has or is perceived to have taken place or the member of staff feels under threat. The purpose behind the use of this equipment is to prevent and detect crime and prevent public disorder. When information is captured, it will firstly be assessed as to whether it constitutes evidential or non-evidential material. Any material, which is deemed as evidential, could then be shared with the Police. On rare occasions BWV material could be released, by the Police, to the media if there is a genuine need to do so. For example the identification of an unknown suspect in relation to a serious offence.

3. How will any information be shared with the Prosecution Services, Defence and the Courts?

Any captured information deemed to be evidential, will in the first instance be 'protected' by means of a Master copy being created. This remains an integral part of the process. A Working copy(s) is created and it is this which will be passed to other Criminal Justice partners and Defence and ultimately the Court. In instances of dispute, the Court can require the production of the Master copy. However these stages are likely to be completed by the Police.

4. Is the data processing exempt from legislative privacy protections?

The Trust will only deploy this technology against defined operational requirements will ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing social need. At all stages it will comply with the Data Protection Act and other legislation.

In the case of the Human Rights Act 1998, 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). Information will only be captured and processed to achieve a legitimate aim as detailed above.

5. Will BWV significantly increase the quantity of data captured and processed in respect of that held on any one individual or a wider group?

BWV is relatively new technology and is seen to have major benefits of capturing evidence in an indisputable fashion. Accordingly, there will be more data potentially being captured but safeguards, will ensure that only information that passes a strict test, of being required for stated purposes, will be retained.

6. What are the safeguards for minimising the retention times for data?

Any information captured on a device, which is deemed to be non-evidential will be automatically deleted after a set period of time (30 days). The rationale for any retention beyond this timescale might include circumstances where there is a desire to review allegations made under the Trust's complaints procedure. Complaints are more often reported in the aftermath of an incident and this material may not have been marked for retention.

Other data within the evidential category will be retained in order to satisfy the requirements of legislation, the court process if applicable and depending on the type of offence retained, reviewed and disposed of. Any onward retention by the Police will be in compliance with their policies. The Trust's BWV database will be linked to the process relating to the control of documents and records allowing for deletion of BWV data in full compliance with the Trust's retention policies.

7. What are the procedures for dealing with the loss of any BWV devices?

It is possible that in some circumstances, such as within a public order or violent encounter, a device might become detached from a staff member and fall into the hands of the wrong person. This privacy risk is limited due to the encryption of the data held on the BWV device. Access to the encrypted data stored on the device's internal memory requires a bespoke docking facility, and associated software which is not widely available.

The means of attaching equipment to the uniform of staff has been subject of much consideration and is designed to physically reduce instances of the equipment being ripped off. The Trust has adopted a process where the devices are booked in and out at the start and end of duty as well as being personally issued to a very limited number of staff in specialist roles. Accordingly, the impact in terms of any time lost between any loss and notification to the Trust, is kept to a minimum.

Where a device is lost, all possible attempts will be made to identify and notify persons who are subject of information on the device.

8. Audio Recording is a greater infringement of my privacy, how can this be justified?

The inclusion of audio improves the quality of the evidence captured, where the capture of video evidence alone may not be sufficient. In some circumstances, the presence of only video evidence, can fail to adequately provide the full context of an incident or complaint. Another aspect of the inclusion of audio information is that, in some instances, the camera itself may not be pointing in the direction of the main incident but the audio will still be captured. This has the advantage of protecting all parties to ensure that the actions of the staff member were in accordance with the law and Trust policies.

9. Collateral intrusion is a significant risk, how will this be handled?

Collateral intrusion in this context extends to the capturing of the movements and actions of other persons, not involved in an incident, when this equipment is being used. It is inevitable that in some circumstances this will occur, albeit staff are trained to ensure that wherever possible, the focus of their activity is on the person subject of the colleague's attention. In circumstances where citizens are captured in any video or audio information and they are unrelated to any offence under investigation, their identities will be protected and anonymised especially should the matter be presented to a court.

10. Do you need consent to record an individual?

Given the purpose for which Trust staff are using BWV, there is no requirement to obtain the consent of the person or persons being filmed. In the event that someone requests that the BWV be switched off, the staff member should advise the person that:

- *Any non-evidential material is only retained for a maximum of 30 days.*
- *This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law.*
- *Recorded material can be accessed on request in writing in accordance with the DPA, unless an exemption applies.*

The BWV operator will consider on a case-by-case basis whether or not to switch the BWV off. There should always be a presumption to record if the 'need to address a pressing social need' has been achieved unless the circumstances dictate otherwise. A colleague failing to record an incident may be required to justify the actions as vigorously as any colleague who chooses to record a like encounter. In all cases, recording can only be justified when it is relevant to the incident and necessary in order to gather evidence.