Privacy Impact Assessment: Body Worn Video

Version: 1.0
Date: May 2017
Author: Head of Information Management
Owner: Chief Superintendent Mike Fawcett

NORFOLK CONSTABULARY
Our Priority is You

SUFFOLK CONSTABULARY
Taking pride in keeping Suffolk safe

Document Control

Sign-Off Details			
Sign-Off Authorities	**Role**	**Date**	**Signature**
Mike Fawcett	Chief Superintendent BWV Project Director	17/05/17	

Distribution List			
Name/Board	**Role**	**Version**	**Date**
K Eade	Compliance Officer – Norfolk/Suffolk Constabularies	Draft 0.1	19.01.2016
H Youngs	Head of Information Management	Draft 0.2	24.11.2016
BWV Project Board	-	Draft 0.3	
BWV Project Board	-	Draft 0.5	
BWV Project Board	-	Draft 0.6	
Publication Scheme	-	Final Version 1.0	18.05.2017

Version Control		
Version	**Date**	**Summary of Changes**
Draft 0.1	19.01.2016	Draft new document
Draft 0.2	24.11.2016	Draft – additional comments following inaugural BWV Project Board 3.7 – 3.8 & 3.15 New paragraph 4.1 – 4.2 New paragraphs Changes to the law surrounding BWV Section 5.13 – Additional stricter guidance controls 5 – Paragraph re-ordering 5.23 – amendment www.ico.org.uk
Draft 0.3	05.11.2016	Various changes without the document based on feedback and/or comments from H Youngs
Draft 0.4	14.12.2016	Various spelling or typo changes made after review by Vicki Cowey
Draft 0.5	12.01.2017	J. Nobbs – Incorporate revisions of paragraphs 3.7, 4.5, 4.11 to reflect views of T/ACC Fawcett. H. Youngs – Incorporate revision of minor changes of T/ACC Fawcett and T/Ch Supt Marshall at 3.5, 4.4. and 4.5. H.Youngs - Inclusion of Annexe 2 – Operating Procedure. Revision of 4.1 to reflect the awarding of contact and Operating Rules. 4.3 to reflect authorisation.
Draft 0.6	07.02.2017	H. Youngs – Incorporate the Body Worn Video Policy into the document.
Draft 0.7	16.05.2017	K. Eade – Update PIA with Consultation Feedback.
Final 1.0	17.05.2017	H. Youngs – Final sign off by the Chair of the BWV Project Board

Contents

List of Annexes –

1. Introduction

1.1. For a number of years, the police service, has undertaken trials on differing types of cameras that are capable of capturing both video and audio information and are collectively known as Body Worn Video (BWV).

1.2. These have been used by uniformed police officers and have either been fitted to their clothing or head mount/ helmet. With the advancement of technology, the devices have become smaller, lighter and more easily carried by officers, which have extended their scope of daily use.

1.3. It is widely known that citizens, going about their daily lives, are likely to have their movements and identity captured on a myriad of surveillance systems and of paramount importance is to mitigate any privacy risks and issues.

1.4. This Privacy Impact Assessment (PIA) has been written to explore these issues and in particular to explain:

- the rationale for Norfolk and Suffolk Constabularies introducing and using this technology;
- the legality behind its use;
- the likely operational circumstances when uniformed officers may use it;
- the key **privacy issues** and **risks** and provides an explanation as to how the organisation mitigates them; and
- how Norfolk and Suffolk Constabularies will continue to monitor the use of the equipment and revisit the Privacy Issues and Risks through ongoing consultation with its community, together with responding to any national and legislative changes.

1.5 This document should also be viewed in the context of the Operational Guide issued to police forces published by the College of Policing.

2. Purpose of a PIA

2.1. Any project or set of new processes that involve exchanging personal information has the potential to give rise to privacy concerns from the public. A Privacy Impact Assessment (PIA) is a flexible process which assists organisations in identifying and minimising the privacy risks of new projects or policies. Conducting a PIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks. A PIA will help to ensure potential problems are identified at an early stage and benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.

2.2. A Privacy Impact Assessment will aim to incorporate the following process:

- Identify the need for a PIA
- Describe the information flows;
- Identify the privacy and related risks;
- Identify and evaluate the privacy solutions;
- Sign-off and record the PIA outcomes
- Integrate the PIA outcomes into the project plan, and
- Consult with internal and external stakeholders as needed throughout the process.

2.3. **What is meant by privacy?**

The Information Commissioner's Office (ICO) *Conducting Privacy Impact Assessment Code of Practice*[1] describes privacy in the following way:

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy – the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

[1] The Information Commissioner's Office (ICO) *Conducting Privacy Impact Assessments Code of Practice* – Page 6

- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

The Privacy Impact Assessment is a process which helps organisations to anticipate and address the likely privacy impacts of projects, in order that problems can be foreseen and solutions developed to ensure that concerns are addressed appropriately.

2.4. Norfolk and Suffolk Constabularies are introducing the use of cameras that are capable of capturing both moving images and audio information and will be worn by police officers and potentially a select number of police staff, inclusive of PCSOs. The devices will be used in a number of policing situations and the aim of undertaking this PIA is to explain the extent of:

- their use;
- their limitations;
- how any data captured will be processed; and
- an analysis of the rights to privacy of citizens and the risks that this could impose on its introduction.

2.5. Finally, this PIA only addresses the application of this equipment in an overt policing capacity.

2.6. The Conducting Privacy Impact Assessments - Code of Practice, launched by the Information Commissioner's Office (ICO) in February 2014 has been used to support this PIA.

3. Structure of this Document

This document explains:

- The aims and benefits of the project and how the project intends to alleviate any public concerns for the use of Body Worn Video as relatively new technology.
- How the steps from the Information Commissioners Conducting Privacy Impact Assessments Code of Practice have been addressed, including:

  Step 1 – Identify the Need for a Privacy Impact Assessment (PIA)
  Step 2 – The Information Flows and Consultation Requirements
  Step 3 – The Privacy and Related Risks
  Step 4 – The Privacy Solutions
  Step 5 – Sign Off of PIA Outcomes
  Step 6 – Integrate the PIA into the Project Plan

Documentation supporting the PIA is contained as Annexes, including:

Annexe 1 – Data Protection 8 Principles
Annexe 2 – Joint BWV Policy
Annexe 3 – Glossary of Terms
Annexe 4 – References & Legislation

What is Body Worn Video (BWV)?

3.1. Any style of camera deployed by the police, which is carried or fixed to the uniform of a police officer or police staff and is capable of capturing both video and audio information collectively falls under the category of BWV.

3.2. The equipment has been in use by some forces for a number of years but with advancing technology, the devices have become smaller, lighter, more easily carried by officers and have far greater capabilities in when and where they can be used. In addition, the actual quality of the captured data is now of a high standard.

3.3. The devices themselves are generally mounted on an officer's uniform or a firearm head unit whereas some of the early models were mounted on officer's heads or their headwear. The equipment will be used in overt policing activities by police officers and police staff.

3.4. **Why use BWV?**

3.5. The Police have a responsibility to maintain law and order; to protect members of the public and their property, and prevent, detect and investigate crime. This involves stopping and speaking to the public and recording information in their pocket notebooks (PNBs). In some instances, the rigour of what has been recorded has been the subject of interpretation and the subject of debate. Equally it may not have presented the best possible primary evidence to support a prosecution. By the introduction of this type of technology, the devices themselves are able to record factual information such as what was said and when, in an indisputable format. Their use will be at the discretion of an officer and should be:

- Incident specific
- Proportionate
- Legitimate
- Necessary; and
- Justifiable

3.6. As mentioned above, police officers have traditionally used their PNBs to record key information, when dealing with a member of the public or capturing initial information at an incident. BWV must be seen as being complementary to an entry being made in the PNB and is not a replacement for it.

3.7. There is an expectation from Norfolk and Suffolk Chief Officers that users will record the following incidents:

- When attending Domestic Abuse or suspected Domestic Abuse incidents.
- Where a user gives a direction to an individual or group under any statutory power.
- When a user decides to use statutory powers to stop a motor vehicle in order to engage with one or more of the occupants.
- When users attend premises in order to affect an arrest.
- Prior to entering any land, premises, vehicle, vessel or aircraft in pursuance of any legal power in order to search those premises and for the duration of the search.
- When a user stops a person in a public place in order to ask them to account for their actions in order to establish their possible involvement or otherwise in an offence.
- When a user decides to conduct a search of a person, premises, land, vehicle, vessel or aircraft in accordance with PACE code A or any other statutory search power.
- When attending Critical Incidents.
- Where a user exercises the use of force against persons or property.

3.8. If a user does not use BWV to record one of the above incidents that are evidential, it is likely to require explanation therefore the rationale should be captured in the evidential statement made by the officer.

3.9. This equipment may therefore be used to record video and audio information of encounters between the police and the public, after ensuring appropriate safeguards in respect of the necessity, legitimacy and legality are addressed in respect of:

- the prevention and detection of categories of crime;
- reduce incidences of public disorder;
- present evidence to the Crown Prosecution Service to bring successful prosecutions before the courts; and
- work to address issues associated with the transparency of police practices.

3.10. Based on the earlier comment above, the following categories of citizens are likely to have their contact, with police officers, recorded:

- victims of crime;
- witnesses of crimes; and
- persons suspected of committing offences.

3.11. In addition, persons, unrelated to any specific interaction between police officers 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 what is seen or heard. In such circumstances, Norfolk and Suffolk Constabularies has adopted a number of safeguards to firstly avoid this where possible and to then follow a number of arrangements to anonymise any data.

3.12. 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 the circumstances at that time. This will not replace the needs to capture other types of evidence but will go a considerable way in reducing any ambiguities and should be considered as an additional policing aid.

3.13. BWV will not be routinely recording and monitoring all activity on a continuous basis. To do so would fundamentally breach the privacy of large swathes of the public, who are going about their legitimate lives, as well as the privacy of officers going about their work. This cannot be justifiable from the perspective of proportionality and legitimacy. Added to this, is that current technology in incapable of operating such a way principally due to a lack of suitable battery life. In addition, such a practice would require the storing, reviewing and then disposal of large quantities of data.

3.14. BWV will only be used by authorised persons who have completed the mandatory training package. Use of BWV will be driven by the incidents and circumstances presented to users or in anticipation of responding to a reported and unfolding incident, or when exercising a specific police power.

3.15. BWV trials that have taken place in other forces have concluded that:

- BWV can reduce the number of vexatious complaints against officers
- There was no overall impact on the number of stop and searches conducted
- There was no effect found on the proportion of arrests for violent crime
- There was no evidence that BWV affected the way that police officers dealt with victims or suspects, and
- In general, communities/local residents are supportive of BWV.

4. General Operating Procedures

4.1. Norfolk and Suffolk Constabularies have awarded the contract for the BWV technology which is being overseen by the BWV Project Board. The detail on how BWV will operate is attached at Annexe 2 – Joint Body Worn Video Policy.

4.2. Norfolk and Suffolk are cognisant to the benefits of BWV implementation due to widespread liaison with forces regionally and nationally. The need to ensure that officers and staff are equipped with the tools required to police efficiently, effectively and in a transparent manner will be supported an enhanced through the delivery of BWV.

4.3. After completing training, officers will be authorised to receive one of these devices at the start of the period of duty. These devices will either be allocated on a personal basis or "booked out" to them from a pool of devices. A set of operational procedures issued by the Constabularies at Annexe 2 will govern the operational use of the devices.

4.4. If a device is lost at any time, a user will report this immediately to a supervisor. All data stored on devices are encrypted to prevent unauthorised access. If a device was obtained by a third party they would be unable to upload or view any footage stored on the device.

4.5. During the course of their normal patrol, the device remains in an inert state and therefore is not recording any material. In order to start recording, officers need to deliberately activate the device to a record mode and where practicable, make a verbal announcement to indicate that the BWV equipment has been activated. This announcement should be present on the recording if possible. Additionally the device will alert the user and the subject of the recording that a recording is taking place via a flashing red light. If practicable this announcement should be present on the recording and if possible, should include:

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

4.6. If the recording has commenced prior to their arrival at the scene of an incident the officer should, as soon as is practicable, announce to those persons present that recording is taking place. Announcements should be made using basic language that can be easily understood by those present. At the conclusion of any incident, the recording mode on the device is switched off and the captured information is stored.

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

4.8. Subject to individual force procedures, the recording of incidents may or may not be concluded when the user moves to another area, such as a Police Investigation Centre, where other video recording systems are able to take over the recording.

4.9. 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:

- Location
- The reason for concluding the recording.

4.10. At the end of a period of duty, the officer or member of police staff returns the device to his/ her station. A process will be in place which involves 'checking in' the device, 'docking' it into a dedicated port and downloading all captured information to a central repository on premise. This information cannot be deleted or altered. The officer will then identify the elements of any captured data that is to be retained to assist in an investigation, and 'mark' the section appropriately, by using the built-in software.

4.11. Once the above process is completed, the contents on the device are erased. Any material required to support an ongoing investigation or prosecution will be retained as fulfilling a 'policing purpose', and will be processed under the **Home Office/ NCPE (2005) Code of Practice Management of Police Information guidance (MoPI) College of Policing (2013) APP on Information Management** as well as the Criminal Procedures Investigations Act 1996 (CPIA). In addition to this, non-crime traffic offences will be stored for 12 months.

4.12. All other material will be automatically erased after a pre-determined timeframe (31 days). Access to recordings will be fully controlled and auditable and only persons having an operational or need to view specific incidents may view do so.

4.13. Where information is captured for use in any investigation, once downloaded, a master copy *(a bit-for-bit copy of the original recording, which is stored securely, pending its production {if required} at court as an exhibit)* of the entire information will be created and a working copy *(the version produced from the original media for the investigation, briefings, circulation and preparation of prosecution evidence and defence)* of this is then made available.

4.14. Any information shared with the Crown Prosecution Service for the purpose of determining any advice/ charge and then to assist in any prosecution, will be strictly controlled in accordance with the **Crown Prosecution Service (2013) The Director's Guidance on Charging 5th Edition**.

4.15. In order that BWV evidence is admissible in court, Norfolk and Suffolk Constabularies follows the principles contained in the **ACPO/ Home Office (2007) Digital Imaging Procedure v2.1** and the **ACPO (2007) Practice Advice on Police Use of Digital Images**.

5. The Law Surrounding BWV

5.1. The use by the police of BWV must be shown to be proportionate, legitimate, necessary and justifiable, in such circumstances where it is necessary in order to gather evidence. In addition, use of the equipment should address a 'pressing social need' especially in respect of its application within the confines of the Articles enshrined by the European Convention of Human Rights within the Human Rights Act 1998. This next section explains the various aspects of the legislation and guidance that covers this equipment, and Norfolk and Suffolk Constabularies will ensure that the rights and privacy of the public are balanced against the law.

It is fully acknowledged that there will be some circumstances where the use of BWV, especially within a private place, is likely to raise special concerns over privacy. The police have to demonstrate in such circumstances that they are addressing a 'pressing social need' by using the equipment since this is 'interference' under the legislation. An exhaustive list of such circumstances cannot be prepared but an example would be incidents and investigations into reports such as domestic abuse. In these instances, particularly where users enter a private place, the use of BWV can provide compelling and corroborative evidence which ordinarily cannot always be adequately conveyed through solely written statements. It is therefore complementary in that it is capable of providing the best possible evidence to capture any comments, demeanour and overall appreciation of the scene and in many instances has been held to be critical evidence in terms of protecting persons.

5.2. **Legality Under Common Law**

5.3. It is accepted, following the provision of legal advice, that the police are able to rely on the fact that the use of BWV is deemed to be lawful under Common Law. Police officers are also held to be 'citizens in uniform' although granted additional statutory powers in order to execute their duties. In addition, police officers generally do not require special statutory powers to undertake any activity that the public could lawfully undertake. An example of this is where a police officer speaks to a person and asks them to account for their actions or conduct. The person does not have to co-operate or stop (*R (Diedrick) v Chief Constable of Hampshire [2012]*).[1]

[1] R (Diedrick) v Chief Constable of Hampshire [2012] EWHC 2144 (admin) at [9]

5.4. The taking of photographs, and in its wider sense video or sound recordings, is deemed lawful and Common Law does not prevent this activity in a public place (Lord Collins in *Wood v Commissioner of Police for the Metropolis [2009]*)[1] (*Murray v the UK [1995]*).[2]

5.5. **Human Rights Act 1998 (HRA)**

5.6. For the purposes of the European Convention of Human Rights (ECHR) and the Human Rights Act 1998, it has been determined that police officers have sufficient powers in common law to justify the use of BWV as above (*Wood v Commissioner of Police for the Metropolis [2009]* and *Murray v the UK [1995]*), however use of BWV is viewed as 'an interference'[3] and must always be justifiable. Therefore any actions by the police must have a legitimate aim and the use of this equipment must be shown to be proportionate to achieving this.

5.7. Under this legislation, a number of 'Articles' protect the rights of citizens. Some of these Articles are absolute whereas others are 'qualified' and any interference with these is limited. Interference with qualified rights is permissible only if:

- There is a clear legal basis for the interference with the qualified right that people can find out and understand, and
- The Action/ Interference seeks to achieve a legitimate aim. Legitimate aims are set out in each Article containing a qualified right and they vary from Article to Article, they include for example, the interests of National Security, the prevention of disorder or crime and public safety. Any interference with one of the rights contained in Articles 8-11 must fall under one of the permitted aims set out in the relevant Article.
- The action is necessary in a democratic society. This means that the action or interference must be in response to a pressing social need and should be assessed by demonstrating evidence of a level of severity or immediacy/ unpredictability, and alternatives should have been reviewed.

5.8. The use of BWV must comply with all the Articles of the HRA, and there are two particular Articles that are critical and most likely to be challenged:

- Article 8 of the ECHR is the right to respect for private and family life, home and correspondence.

[1] R (on the application of Wood) v Commissioner of Police for the Metropolis [2009] EWCA Civ 414 at [98]
[2] Murray v UK [1995] 19 EHRR 193
[3] Ben Jaffey QC December 2013

Under the legislation, this Article is a qualified right and, Police forces are required to consider this Article when dealing with recorded images, whether they are made in public or private areas. Accordingly, this assessment looks to address the issues raised by this Article and introduces suitable safeguards, associated with how Norfolk and Suffolk Constabularies deploy this equipment, in both the public and private arenas, and then how we deal with the product from any use. Throughout, the principle objective is ensuring that any interference with the rights of parties can only be justified if it is:

- **Necessary**
- **In pursuit of a legitimate aim** – such as the prevention, investigation and detection of crime, with the necessity test being satisfied by the presence of a pressing social need.
- **In accordance with the law** – legal advice has been sought to establish that BWV is in accordance of the law.

- Article 6 of the ECHR provides for the right to a fair trial.

5.9. 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.

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

5.11. Recordings of persons in a public place are only public for those present at the time, so those situations are therefore still regarded as potentially private (*R v Brentwood Borough Council ex parte Peck [2003]*)[1]. Recorded conversations between members of the public should always be considered private.

5.12. Users of BWV must consider Article 8 when recording and must not record beyond what is necessary for policing purposes.

[1] Peck v United Kingdom [2003] 36 EHRR 41; [2003] EMLR 28

5.13. BWV should only be used in such circumstances where it is strictly necessary in order to gather evidence, and there is no other reasonable means of gathering the necessary evidence.

5.14. It is fully acknowledged that there will be some circumstances where the use of BWV, especially within a private place, is likely to raise special concerns over privacy. The police have to demonstrate in such circumstances that they are addressing a 'pressing social need' by using the equipment since this is 'an interference' under the legislation. An exhaustive list of such circumstances cannot be prepared but examples could likely include incidents and investigations into reports such as involving violence or abuse within a domestic environment but even then should only be used when alternative means of obtaining the quality and conclusive standard of evidence, have been considered and discounted. In these instances, particularly where officers enter a private place, the use of BWV can provide compelling and corroborative evidence which ordinarily cannot always be adequately conveyed through solely written statements. It is therefore complementary in that it is capable of providing the best possible evidence to capture any comments, demeanour and overall appreciation of the scene and in many instances has been held to be critical evidence in terms of protecting persons.

5.15. Norfolk and Suffolk Constabularies will impose stricter guidelines where BWV is being used in places not open to the public or where a person is being recorded would have a strong expectation of privacy. These include:

Private Residence

When dealing with incidents in private residence, especially at a time of day when people are likely to be in bed, users must be able to justify use of BWV against this expectation of privacy. Unlike in public places, the user must be acting in the lawful execution of their duty to use BWV whilst in a private residence. Users will balance the privacy needs of the individuals against the benefits that use of BWV provides. It is clear that BWV provides excellent evidence in the investigation of Domestic Abuse and can assist in evidence based prosecutions against offenders, where previously no further action would be taken.

Toilets/Changing facilities

Users are aware of the higher threshold of justification that is required for use of BWV in areas such as toilets, changing rooms or any other circumstances where they may come across persons in a state of undress.

Intimate Searches

BWV will not, under any circumstances, be used for recording intimate searches or in any other circumstances where persons are in a state of undress.

Legal Privilege

Users will respect legal privilege and must not record material that is, or is likely to be, subject to such protections.

Journalistic Material

This equipment will not be used in any way in which it is likely to collect journalistic material.

Likely to Cause Serious Offence

Care should be exercised in using BWV where it may cause serious offence, for example during a religious ceremony. Users must have an increased justification to use BWV against this expectation of privacy.

Formal Interviews

BWV should not be used for formal investigative interviews e.g. the Achieving Best Evidence interview for evidence in- chief purposes, or a significant witness interview for the purpose of preparing a statement. The use of BWV for the interview of suspects is not permitted as it would be in contravention of **PACE Code C** and it is currently unsuitable for recording interviews with vulnerable or intimidated witnesses and victims.

5.16. Norfolk and Suffolk Constabularies will continue to monitor all use of this equipment to ensure that it remains proportionate. Additionally the Constabularies will update the PIA process if their findings warrant any change.

5.17. **Data Protection Act 1998**

5.18. The Data Protection Act 1998 (DPA) is legislation that regulates the processing of personal data including sensitive personal data, whether processed on a computer, CCTV, stills camera or any other media. Any recorded image and audio recording from any device, which includes BWV, that can identify a particular person or learning about their activities, is described as personal data and is covered by the DPA and in particular within the principles contained within, a full list of which are included as an appendix;

5.19. Principle 1 of the DPA (Fair and Lawful Processing) requires that you must:

- have legitimate grounds for collecting and using the personal data;

- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

5.20. Norfolk and Suffolk Constabularies have the responsibility for controlling this information and are known as Data Controllers for information captured and used within their areas, for a policing purpose. If required, a police officer or police staff using a BWV device must be prepared to explain how the capture and processing of any data is compliant with the legal obligations imposed under this Act.

5.21. In order for Norfolk and Suffolk Constabularies to ensure compliance with the DPA, the following has been undertaken:

- local media engagement to advertise the use of BWV, using local newspapers and other media and the websites for both forces;
- advice provided to the local community-based forums of the use of this technology in their area;
- ensuring that users where possible/ practicable, announce to the subject(s) of the encounter that video and audio recording is taking place using BWV.

5.22. The sharing of BWV images with other agencies and the media, and any images will only occur in accordance with the requirements of the Act.

5.23. For further information relating to the DPA, please see **the College of Policing (2013) APP on Information Management** and the website of the **ICO** at www.ico.org.uk.

5.24. **Criminal Procedure and Investigations Act 1996**

5.25. The Criminal Procedure and Investigations Act 1996 introduced the statutory test for disclosure of material to the defence in criminal cases.

5.26. Norfolk and Suffolk Constabularies are able to disclose both used and un-used images and demonstrate that this has been done. Deletion of any police-generated images (or a third party's images in police possession) prior to their respective retention periods, may amount to a breach of the Act if they are not then available for disclosure. Images that are relevant to

an investigation must be retained in accordance with the Code of Practice issued under Section 23 of the CPIA.

5.27. The **ACPO (2007) Practice Advice on Police Use of Digital Images Section 1.2 Criminal Justice Disclosure** contains further information about this requirement. Police generated digital images should be accompanied by a full audit trail, from the point of capture of the image throughout the whole management process – including when they are passed to the CPS or the defence or if there is any supervised viewing.

5.28. **Freedom of Information Act 2000**

5.29. The Freedom of Information Act 2000 grants a general right of access to all types of recorded information held by public authorities, which includes digital images recorded by BWV. The Act does however provide some specific exemptions to the requirements to disclose information.

5.30. **Protection of Freedoms Act 2012 & the Surveillance Camera Code of Practice**

5.31. Part 2 of the Protection of Freedoms Act 2012 deals with the regulation of CCTV and other surveillance camera technology and introduces the Code of Practice for Surveillance Camera systems. Section 29(6) of the act provides that this code covers "any other systems for recording or viewing visual images for surveillance purposes". This would include BWV.

5.32. Norfolk and Suffolk Constabularies adhere to this code as its content will be relevant when a court is considering whether the use of BWV:

- complies with the first Data Protection Principle;
- is prescribed by law for the purposes of Article 8 ECHR; and
- is a proportionate interference with Convention Rights under Article 8(2) ECHR.

5.33. **Home Office/ NCPE (2005) Code of Practice on the Management of Police Information (MoPI)**

5.34. This consists of both guidance and a Code of Practice that directs how the Police Service will handle any data that comes into its possession. Data, which includes information from a BWV device, can only be retained for a 'police purpose' and this covers all situations where a police officer exercises a police power, where they would have ordinarily made a record in their pocket notebook, or there is a strong and reasonable presumption toward the collection/ capture of evidence.

5.35. There may be occasions where a police officer wishes to record an encounter to evidence their own actions; there must be a legitimate reason to this decision, and the recording cannot be used for the sole purposes of aiding the identification of an individual, in that this has been held to be unlawful[1]. The decision to record in these circumstances needs to be taken in line with the principles of data management and record retention and the provisos contained within this assessment. Officers should be prepared to account for their decision-making in such instances.

5.36. The guidance further states that a Policing Purpose includes:

- Protecting Life and Property
- Preserving Order
- Preventing the Commission of Offences
- Bringing Offenders to Justice
- Any Duty or Responsibility of the Police Arising from Common Law or Statute.

5.37. These five purposes provide the legal basis for collecting, recording, evaluating, sharing and retaining police information.

5.38. The guidance provides a framework on how any data captured by the police can be used and processed. In addition, it details the process to be used by the police service to initially retain information, to review this and to when to ultimately dispose of data after requisite timescales and circumstances. In addition the **College of Policing (2013) APP on Information Management** contains useful additional information.

[1] Wood v Commissioner of Police for the Metropolis [2009] EWCA Civ 414

6. Step 1 - Identify the Need for a PIA

6.1. In accordance with the ICO Code of Practice, an assessment was carried out to determine if a PIA was necessary using the following screening questions:-

- **Does the project involve multiple organisations whether they are government agencies or private sector organisations?**

  No. At present the intention is that BWV will only be used by police officers and police staff from Norfolk and Suffolk Constabularies.

- **Does the project involve new or significantly changed handling of personal data that is likely to raise privacy concerns with individuals?**
  The project does not involve new or significantly changed handling of personal data however there will be operating procedures will be created to ensure compliance with all relevant legislation and best practice recommendations.

- **Does the project involve new or significantly changed handling of a considerable amount of personal data about individuals?**
  The constabularies are not significantly changing the way in which they handle personal data; however the volume of this type of data captured by the organisations is likely to increase.

- **Will the project use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**
  No.

- **Will the project compel individuals to provide information about themselves?**
  No, the devices will act as a supplementary tool for evidence capture alongside traditional methods.

- **Will the information about individuals be disclosed to organisations or people who have not previously had routine access to information?**
  No.

- **Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**
  Yes. Better quality evidence is hoped to result in a higher rate of convictions and increase the opportunity for early guilty pleas. In addition the number of vexatious complaints is hoped to be reduced following the implementation of BWV.

- **Will the project require you to contact individuals in ways that they may find intrusive?**
  No

- **Does the project involve you using new technologies which might be perceived as being privacy intrusive?**
  Yes. It is understandable that members of the public and other organisations may perceive the use of BWV to be intrusive. However all relevant legislation and guidance will be adhered to, in addition to the enforcement of measures in circumstances that of a particularly sensitive nature (e.g. Female Genital Mutilation and Honour Based Abused).

- **Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?**
  No

- **Does the project relate to data processing which is in any way exempt from legislative privacy protections?**
  Yes – some exemptions may apply e.g. S29 (Crime and Taxation) / S35 (Disclosures required by law).

- **Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?**
  No. All parties (such as CPS) that are to have access to BWV footage are subject to the same or comparable privacy regulations.

7. Step 2 - Information Flows

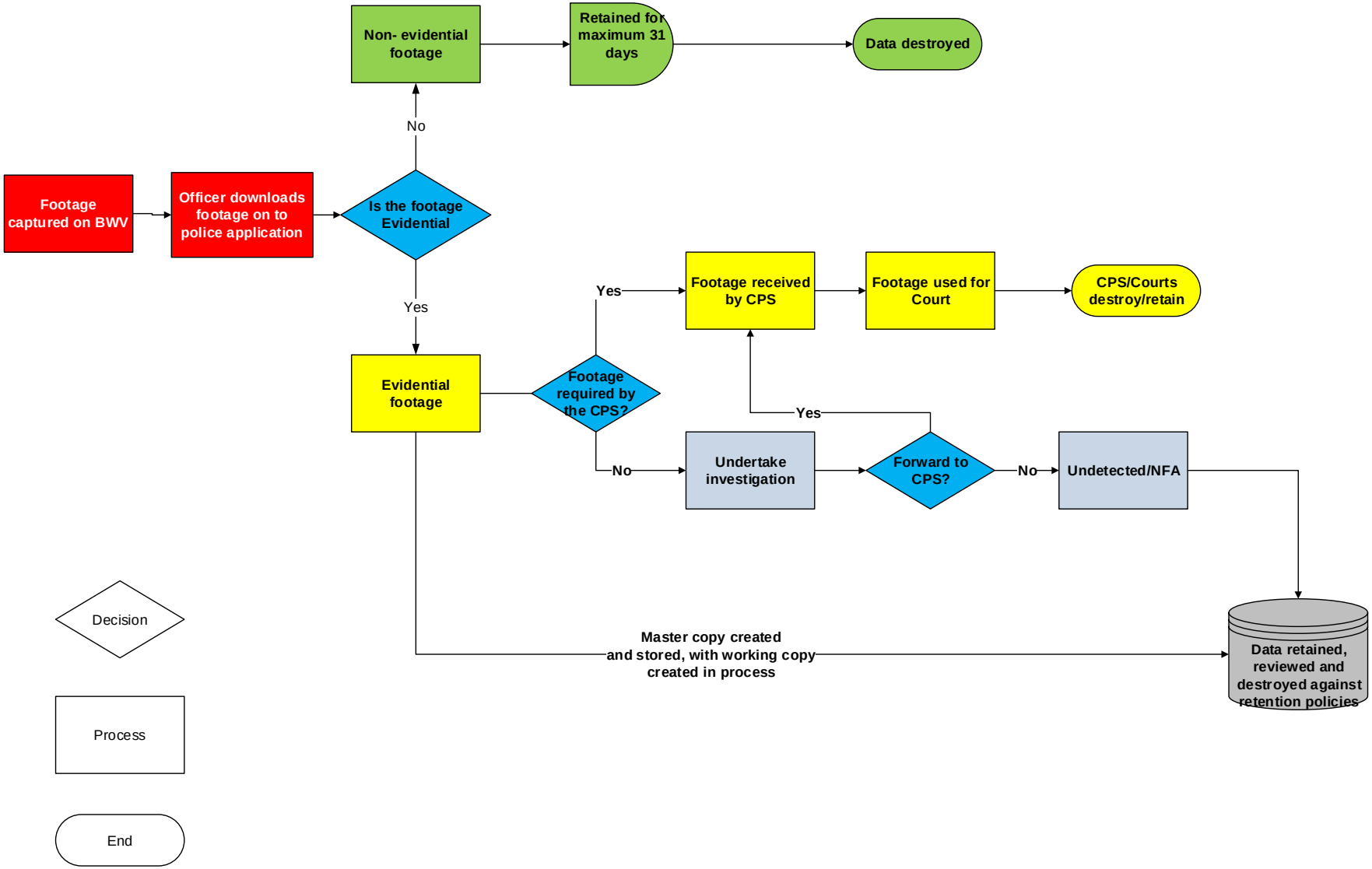
7.1. The chart below demonstrates, in simple terms, how information captured on a BWV device is captured, processed and then disposed of. Norfolk and Suffolk Constabularies respectively have the responsibility for the processing of information in its possession which commences at the point when an officer captures it.

7.2. Clearly, when information is identified as being non-evidential, this follows a process whereby it is automatically deleted after a short determined timeframe of 31 days.

7.3. In circumstances where the information is evidential, master and working copies are created and retained. At the conclusion of any investigation, there is a requirement to hold the data strictly in accordance with MoPI requirements which detail specific time frames based on the nature of the offence/incident, and includes undertaking appropriate reviews, further retentions if appropriate and then disposal.

7.4. Where information is shared with the CPS, Norfolk and Suffolk Constabularies no longer have the responsibility for the shared data and the retention timeframes and disposal requirements then revert to that organisation.

7.5. The collection of data is the start of the information management process. It affects all other stages of information management, from how the information is recorded to how long it will be retained. It is essential that information is collected, recorded and evaluated in a consistent manner across organisational and force boundaries. The College of Policing has published the Information Management Authorised Professional Practice (APP) to assist forces with their data collection and recording responsibilities, which can be found at: http://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/.


Non- evidential footage
Retained for maximum 31 days
Data destroyed
No
Footage captured on BWV
Officer downloads footage on to police application
Is the footage Evidential
Yes
Yes
Footage received by CPS
Footage used for Court
CPS/Courts destroy/retain
Evidential footage
Footage required by the CPS?
Yes
No
Undertake investigation
Forward to CPS?
No
Undetected/NFA
Master copy created and stored, with working copy created in process
Data retained, reviewed and destroyed against retention policies
Decision
Process
End

8. Step 3 – Privacy and Related Risks

8.1. Through the introduction of this type of technology, there might naturally be concerns associated with how any information is being captured, processed and retained by Norfolk and Suffolk Constabularies. The purpose of this section is to firstly identify what these issues are and to then provide an explanation of the mitigation that Norfolk and Suffolk Constabularies will apply, to ensure the risks are kept to a minimum.

Privacy Issue	Privacy Risk Mitigation
BWV introduces new and additional information technologies that have a substantial potential for privacy intrusion.	BWV is a relatively new technology being deployed by Norfolk and Suffolk Constabularies. However, both forces recognise the concerns from the public regarding privacy issues. Accordingly, this technology will only be deployed in an overt manner, using trained 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 1998, and retained and subsequently disposed of in accordance with the Management of Police Information guidance and Codes of Practice.
BWV technology allows information to be shared with multiple agencies?	When capturing information on these devices, police officers will only do so in order to fulfil a policing purpose. The legitimate policing 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 Crown Prosecution Service, Defence professionals and the Courts to support a prosecution.
How will any information be shared with the Crown Prosecution Service, 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 any dispute, the Court can require the production of the Master copy.
Is the data processing exempt from legislative privacy protections?	Norfolk and Suffolk Constabularies will only deploy this technology against the defined operational requirements & to ensure that the use is proportionate, legitimate, necessary and justifiable. In addition, it will ensure that 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) & 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 & processed to achieve a legitimate aim as detailed.

Will the handling of any data change significantly to be of concern?	The police currently capture digital evidence from CCTV systems and other mechanisms and process this in accordance with legislation and strict codes. BWV provides another source of information, but there are a number of significant differences. Firstly this technology allows the capture of both video and audio data which differs from CCTV but a principle issue is that without the introduction and adherence to essential safeguards, there is the greater risk of the possibility of widespread intrusions into the privacy of citizens. However there are appropriate policies and legislative requirements imposed on its use, and Norfolk and Suffolk Constabularies are confident that these will minimise this risk.
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 a 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 the appropriate safeguards, by adherence to legislation and guidance, will ensure that only information that passes a strict test, of being required for a police purpose, can be retained. BWV will additionally be used during the policing of public order events in which it will capture information about a wider group.
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 31 days. The rationale for any retention beyond an immediate disposal might include circumstances where there is a desire to review any allegations as part of the police complaint procedure, the reporting of these more often occurring the aftermath of any incident and often this material may not have been marked as evidential. 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, in accordance with timeframes within the Home Office/NCPE (2005) Code of Practice on the Management of Police Information and College of Policing (2013) APP on Information Management.
What are the procedures for dealing with the loss of any BWV devices?	Due to the very nature of policing, it is possible that in some circumstances, such as within a public order or violent encounter, a device might become detached from an officer and fall into the hands of persons and therefore potentially lost with the possibility of the data being accessed by an unauthorised individual. The means of attaching equipment to the uniform of police officers has been subject of much consideration and is designed to physically reduce instances of the equipment being ripped from an officer. Devices will either be issued on a personal basis or booked out to an individual from a pool of devices. As such, the impact in terms of any time lost between any actual loss and notification to the forces, 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. The limited amount of captured information is stored on the device's internal memory and requires specific docking facilities to access the footage.
Audio Recording is a greater infringement of my privacy, how can this be justified?	As previously stated BWV is a new technology and is seen to have major benefits of capturing evidence in an indisputable fashion. In order to ensure that all aspects of an incident are captured, this requires the essential inclusion of audio information in order for this to be complementary to the video data. The other important aspect of the addition of audio information is that in some instances, the camera itself may not be pointing in the direction of the main incident but that the audio will still be captured. This has a significant advantage of protecting all parties to ensure that the actions of the police were totally in accordance with the law and addresses issues of police transparency. Equally, in some instances, 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.
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 when this equipment is being used. It is inevitable that in some circumstances this will occur, albeit officers are trained to ensure that wherever possible, the focus of their activity is on the person subject of the officer's attention. In circumstances where individuals 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.
Do you need consent to record an individual?	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 police are deemed to be lawful. In the event that someone requests that the BWV be switched off, the police officer should advise the person that: • Any non-evidential material is only retained for a maximum of 31 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; and • Recorded material is police information and that it can be accessed on request in writing in accordance with the Data Protection Act 1998, unless an exemption applies in the circumstances (Data Protection Act 1998 – Section 7: Subject Access). The police officer 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. An officer failing to record an incident may be required to justify the actions as vigorously as any officer 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.
Are you allowed to record in private dwellings?	It is widely recognised that citizens are likely to have a strong expectation of privacy especially in their own homes. Indeed this is contained with Article 8 of the ECHR (a right to respect for a private and family life) and under normal circumstances BWV should not be used in private dwellings. However if the user is present at an incident in a private dwelling, there is a genuine policing purpose and this equipment is able to address a 'pressing social need' then the police can consider making a BWV recording in the same way in which any other incident is recorded. The user will be mindful to exercise discretion and recording should only be used when it is relevant to the incident and necessary in order to gather evidence, where other reasonable means of doing so are not available. All recordings require a lawful basis in order to justify infringement of Article 8. In circumstances where an occupant of the premises objects to the recording taking place but where an incident is taking place or allegations of a criminal nature are being made, police officers are recommended to continue with a recording but explain their reasons for doing so. These reasons might include: • That an incident has occurred requiring police to attend • That the police officer's continued presence might be required to prevent a breach of the peace or injury to any person • There is a requirement to secure best evidence of any offences that have occurred and that the video/audio evidence will be more accurate and of a higher quality and therefore in the interests of all parties • That continuing to record would safeguard both parties, with a true and accurate recording of any significant statement made by either party and of the scene • That the incident may reoccur in the immediate future or That continuing to record will safeguard the BWV user against any potential allegations from either party. Norfolk and Suffolk Constabularies are very mindful of the concerns that this raises and will train its users to respect and adhere to these safeguards.

9. Step 4 – The Privacy Solutions

9.1. These will be informed by the consultation process and will be documented after the consultation has been completed.

9.2. Norfolk and Suffolk Constabularies see this element as an essential part in its introduction and use of BWV. It is critical that the organisation continues to retain the trust and consent of the local community. Accordingly, it has completed a communication and consultation programme involving the following organisations, groups and using a variety of communication mediums:

- National Police Chiefs' Council (NPCC)
- Her Majesty's Inspectorate of Constabulary
- Independent Police Complaints Commission (IPCC)
- Police Federation (Norfolk / Suffolk)
- The Police Superintendents' Association
- Unison (Norfolk / Suffolk)
- PCC Offices and Independent Advisory Groups (PCC to act as conduit)
- Information Commissioner's Office (ICO)
- Liberty
- Nacro
- The Equality and Human Rights Commission
- Victim Support
- Government Equalities Officer
- Youth Justice Board
- Age UK

9.3. The below responses were received:

Information Commissioner's Office (ICO) -

2.4. Norfolk & Suffolk Constabularies are introducing the use of cameras that are capable of capturing both moving images and audit information….
Helpful that both data streams, with their different potentials for privacy intrusion, are recognised.

3.2. ...equipment been in use for a number of years, with advancing technology...actual quality of the captured data is now of a high standard.
Meaning that the images are more likely to support the reasons for them being processed, e.g. evidence capture, but the scope for privacy intrusion may well be higher as individuals will be more identifiable, rather than grainy and blurred. Helpful that that this is recognised so that the PIA is really considering what is being recorded.

3.3. The devices themselves are generally mounted on an officer's uniform or head unit...
The positioning of the cameras will have an impact on the range and angle of what can be captured which is relevant as it affects adequacy of processing and privacy intrusion. Presumably this has been considered as the positioning has been covered here. Helpful to drill down into how this affects what is actually recorded.

3.9. This equipment may therefore be used to record video and audio information of encounters between the police and the public, after ensuring appropriate safeguards in respect of the necessity, legitimacy and legality are addressed in respect of: work to address issues associated with the transparency of police practices.
Understood, but I'd recommend more advice to users on where this is likely to be appropriate. There is scope for excessive recording here if there isn't clear direction.

3.11. Capture of data unrelated to specific incident - In such circumstances, Norfolk & Suffolk Constabularies has adopted a number of safeguards to firstly avoid this where possible and to then follow a number of arrangements to anonymise any data.
Good.

3.14. BWV will only be used by authorised persons who have completed the mandatory training package.
Good and it is good practice to monitor the effectiveness of training; refresh it and remind users about compliant use.

3.15. BWV trials that have taken place in other forces…
Is this the MPS pilot? If this is included, would be helpful to show how this maps across to BWV use by Norfolk and Suffolk.

4.4. All data stored on devices are encrypted to prevent unauthorised access.
Good that encryption is in place. Has this been tested?

4.14. Any information shared with the Crown Prosecution Service for the purpose of determining any advice/charge… will be strictly controlled in accordance with CPS Guidance.
Each data should be aware of their responsibilities in ensuring appropriate levels of security in the information flow.

5.15. Norfolk and Suffolk Constabularies will impose stricter guidelines where BWV is being used in places not open to the public…
This section is helpful as it highlights examples of where there are greater expectations of privacy.

5.21. In order for Norfolk and Suffolk Constabularies to ensure compliance with the DPA, the following has been undertaken...
Good - consultation is a key aspect of the PIA process. You could consider listing how you've addressed any concerns that have been raised.

5.32. Norfolk and Suffolk Constabularies adhere to this code (PoFA / Surveillance Camera Code of Practice) as its content will be relevant when a court is considering whether the use of BWV a) complies with the first Data Protection Principle.
i.e. that its use is lawful?

6.1. Screening Questions – (1) Does the project involve multiple organisations whether they are government agencies or private sector organisations? Answer: No. At present the intention is that BWV will only be used by police officers & staff from Norfolk / Suffolk Constabularies.
So, two data controllers. I'm assuming that information sharing agreements are in place that cover this so that there is clarity of responsibility, e.g. when handling SARs, or if there is a data breach?

6.1. Screening Questions – (2) Does the project involve new or significantly changed handling of personal data that is likely to raise privacy concerns with individuals? Answer: The project does not involve however there will be operating procedures will be created to ensure compliance with all relevant legislation and best practice recommendations.
Surely the introduction of BWV does this?

6.1. Screening Questions – (3) Does the project involve new or significantly changed handling of a considerable amount of personal data about individuals? Answer: The Constabularies are not significantly changing the way in which they handle personal data; however the volume of this type of data captured by the organisations is likely to increase.

Again, I'm not clear on why this conclusion has been reached?

6.1. Screening Questions – (7) Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? Answer: Yes. Better quality evidence is hoped to result in a higher rate of convictions and increase the opportunity for early guilty pleas. In addition the number of vexatious complaints is hoped to be reduced following the implementation of BWV.

Would say that this against police officers if that is the case. You may wish to refer to research in this area. However, consider how this connects with: purposes for processing personal data / transparency.

6.1. Screening Questions – (9) Does the project involve you using new technologies which might be perceived as being privacy intrusive. Answer: Yes. It is understandable that members of the public and other organisations may perceive the use of BWV to be intrusive.

How has this been addressed in consultation with the public? What were their views?

6.1. Screening Questions – (11) Does the project relate to data processing which is in any way exempt from legislative privacy protections? Answer: No.

It may well do.

7.2. Clearly, when information is identified as being non-evidential, this follows a process whereby it is automatically deleted after a short determined timeframe of 31 days.

Does this rely on the officer flagging it as such? If so, how will this work in practice?

8.1. Step 3 – Privacy and Related Risks: What are the procedures for dealing with the loss of any BWV devices?

Breach reporting should be part of this process.

8.1. Step 3 - Privacy and Related Risks: Audio Recording is a greater infringement of my privacy, how can this be justified?
Can audio be disabled on the cameras? Also relevant to consider what measures would be in place to mitigate privacy intrusion in situations where there is audio that is unrelated to the primary focus of the recording, e.g. via a radio.

8.1. Step 3 - Privacy and Related Risks: Collateral intrusion is a significant risk, how will this be handled? Answer: In circumstances where individuals 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.
This will also need to be available in order to comply with subject access requests.

8.1. Step 3 - Privacy and Related Risks: Do you need consent to record an individual? Answer: … In the event that someone requests that the BWV be switched off, the police officer should advise the person that ... Recorded Material is police information and that it can be accessed on request in writing in accordance with the, unless an exemption applies in the circumstances. Freedom of Information Act 2000.
Subject access falls under the Data Protection Act (s7).

- Acknowledged and amended.

Annexe 4 – References and Legislation
Please also refer to the ICO CCTV code.

- Acknowledged and amended.

The Equality and Human Rights Commission

Referred to Business Plan 2016/17

Victim Support (Norfolk / Suffolk)

Indecently exposed individuals - what would happen if during an incident, an individual's clothing was torn to the extent they were indecently exposed, or if attending a domestic incident, persons were not properly dressed - would these images by protected by means of pixilation or some other method to protect an individual's dignity when viewed by CPS, Courts, Solicitors etc?

9.4. Norfolk and Suffolk Constabularies will continue to assess any issues or concerns being brought to our attention of from assessments of operational deployments and feedback. Any privacy issues coming to light, will be assessed and where appropriate, addressed through their incorporation in this assessment and if necessary through amendments to our operational deployment policies.

10. Step 5 – Sign-Off of PIA Outcomes

10.1 The first column of the table below sets out the suggested privacy solutions which were identified as a result of the consultation exercise set out in Chapter 7. These were discussed by the Body Worn Video Project Board and the recommendations were accepted by the Board on [date] and as a consequence this finalised document was produced.

Suggested Privacy Solution	View and recommendation of the BWV Project Board	Decision of the BWV Project Board
Camera Position: *The positioning of the cameras will have an impact on the range and angle of what can be captured which is relevant as it affects adequacy of processing and privacy intrusion. Presumably this has been considered as the positioning has been covered here. Helpful to drill down into how this affects what is actually recorded.*	One of the reasons behind the purchase of the BWV solution was due to the oscillating camera lens which enables officers of varying height to adjust for the best field of view.	As stated.
Equipment used to record video/audio information: *Understood, but I'd recommend more advice to users on where this is likely to be appropriate. There is scope for excessive recording here if there isn't clear direction.*	This is addressed within the user training as well as FAQs available to staff.	As stated.
BWV trials: *Is this the MPS pilot? If this is included, would be helpful to show how this maps across to BWV use by Norfolk and Suffolk.*	No this relates to the use of BWV within Bedfordshire, Hertfordshire and Cambridgeshire police forces.	As stated.
Encrypted Devices: *Good that encryption is in place. Has this been tested?*	Yes, this has been part of our operational acceptance testing.	As stated.
Multiple Organisations: *So, two data controllers. I'm assuming that information sharing agreements are in place that cover this so that there is clarity of responsibility, e.g. when handling SARs, or if there is a data breach?*	The Information Management department is a collaborated Department covered by a Section 22a agreement. In the event of data sharing, breaches, SARs, the Department services both forces and administers the process.	As stated.

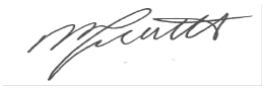
Suggested Privacy Solution	View and recommendation of the BWV Project Board	Decision of the BWV Project Board
	All police forces follow the same national guidance for information management which can be located at College of Policing Authorised Professional Practice: Information Management. There is no requirement for forces to sign Information Sharing Agreements as they are all processing data for crime prevention purposes.	
New or significantly changed handling of personal data: *Surely the introduction of BWV does this?*	BWV footage will be treated in the same manner as the existing capture CCTV footage – in this respect, capturing images is not 'new' processing of personal data.	As stated.
New or significantly changed handling of a considerable amount of personal data: *Again, I'm not clear on why this conclusion has been reached?*	BWV footage will be treated exactly the same as another CCTV such as public space. Whilst the volume will be much higher as the forces, the way in which it is handled remains the same.	As stated.
Significant impact Decision-making: *Would say that this against police officers if that is the case. You may wish to refer to research in this area. However, consider how this connects with: purposes for processing personal data / transparency.*	As complaints are not purely against police we are comfortable with the wording of this.	As stated.
Privacy intrusive new technologies: *How has this been addressed in consultation with the public? What were their views?*	BWV as a technology is used in the majority of police forces across the UK so we have used their learning through public consultation as well as engaging with members of the public through public meetings through the PCC's office. Feedback has been positive as they see the benefits.	As stated.

Suggested Privacy Solution	View and recommendation of the BWV Project Board	Decision of the BWV Project Board
Exemptions from legislative privacy protections: *It may well do.*	Yes – some exemptions may apply e.g. S29 (Crime and Taxation) / S35 (Disclosures required by law).	As stated.
Non-Evidential information deleted after 31 days: *Does this rely on the officer flagging it as such? If so, how will this work in practice?*	No, if the footage is not marked as evidence the system will automatically delete after 31 days.	As stated.
What are the procedures for dealing with the loss of any BWV devices? *Breach reporting should be part of this process.*	There is a process in place for any loss of IT equipment and/or personal data and BWV is no different. There is no way to remotely wipe the devices but strong encryption is implemented there is no way of extracting the data either.	As stated.
Audio Recording is a greater infringement of my privacy, how can this be justified? *Can audio be disabled on the cameras? Also relevant to consider what measures would be in place to mitigate privacy intrusion in situations where there is audio that is unrelated to the primary focus of the recording, e.g. via a radio.*	No audio cannot be disabled on the camera however redaction of the footage (audio and/or video) can be applied post incident if required.	As stated.
Indecently exposed individuals - what would happen if during an incident, an individual's clothing was torn to the extent they were indecently exposed, or if attending a domestic incident, persons were not properly dressed - would these images by protected by means of pixilation or some other method to protect an individual's dignity when viewed by CPS, Courts and Solicitors etc?	Yes - redaction can be applied for these types of incidents.	As stated.

11. Step 6 – Integrate the PIA into the Project

11.1 This section will be completed after sign-off from the Chair of the Body Worn Video Project Board.

On Friday 12th May 2017, the Body Worn Video Project Board proposed recommendations to address the privacy measures raised. The BWV Project Board determined that this Privacy Impact Assessment should be reviewed after a requisite period of time following the implementation of Body Worn Video across Norfolk and Suffolk Constabularies. That review will be initiated by the BWV Project Board.

Signed: 

Name: Mike Fawcett

Position: Chief Superintendent (Chair of the BWV Project Board)

Date: 17th May 2017

Annexe 1

Data Protection Act Principles

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Annexe 2

Joint BWV Policy – Publication Scheme (Policies and Procedures)

Please click on below Links: -

NORFOLK CONSTABULARY
Our Priority is You

SUFFOLK CONSTABULARY
Taking pride in keeping Suffolk safe

Annexe 3

Glossary of Terms

ACPO	Association of Chief Police Officers (Now the NPCC)
BWV	Body Worn Video
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CCTV	Close Circuit television
DPA	Data Protection Act 1998
ECHR	European Convention on Human Rights
FOIA	Freedom of Information Act 2000
HRA	Human Rights Act 1998
MoPI	Management of Police Information
NPCC	National Police Chiefs Council
PACE	Police and Criminal Evidence Act 1984
PIA	Privacy Impact Assessment
PNB	Pocket Notebook

Annexe 4

References and Legislation

The Information Commissioner's Office *Conducting Privacy Impact Assessments Code of Practice*
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

The Information Commissioner's Office Code of Practice for Surveillance Cameras and Personal Information
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Crown Prosecution Service (2013) The Director's Guidance on Charging 5th Edition
http://www.cps.gov.uk/publications/directors_guidance/index.html

ACPO/Home Office (2007) Digital Imaging Procedure v2.1
http://www.bksv.co.uk/ServiceCalibration/Support/UKFaq/~/media/UnitedKingdom/FAQ%20Downloads/DIP_2%201_16%20Apr%2008_v2%203_%20Web.ashx

ACPO (2007) Practice Advice on Police Use of Digital Images
http://library.college.police.uk/docs/acpo/police-use-of-digital-images-2007.pdf

College of Policing (2013) APP on Information Management
http://www.app.college.police.uk/app-content/information-management/?s

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

Criminal Procedures and Investigation Act 1996
http://www.legislation.gov.uk/ukpga/1996/25/contents

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Protection of Freedoms Act 2012
http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Surveillance Camera Code of Practice

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf