West Midlands Police
Privacy Impact Assessment of Body Worn Video

Introduction

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). 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 has extended their scope of use. 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. This Privacy Impact Assessment has been written to explore these issues and in particular to explain:

- the rationale for West Midlands Police 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.
- how West Midlands Police 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.

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

Purpose of Privacy Impact Assessment (PIA)

Any project or set of new processes that involve exchanging personal information, inevitably gives rise to privacy concerns, from the public. Indeed, the cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and government agencies alike.

What is meant by privacy?

The Information Commissioner's Office *Conducting Privacy Impact Assessments code of practice*[1] describes privacy in the following way:

[1] The Information Commissioner's Office *Conducting Privacy Impact Assessments code of practice page 6*

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.*

- *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.

West Midlands Police has introduced the use of cameras that are capable of capturing both moving images and audio information and will be worn by uniformed police officers. The devices will be/have been 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
- an analysis of the rights to privacy of citizens and the risks that this could impose on its the introduction.

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

What is Body Worn Video?

Any style of camera deployed by the police, which is carried or fixed to the uniform of a police officers and is capable of capturing both video and audio information collectively falls under the category of Body Worn Video.

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.

The devices themselves are generally mounted on an officer's uniform whereas some of the early models were mounted on officer's heads or their headwear. The equipment will be used in overt policing activities, in other words by police officers in uniform.

Why use BWV?

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 (PNB's). 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 exactly what happened, 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.

As mentioned earlier, Police officers have traditionally used their PNB's 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 any entry being made in the PNB and is not a replacement for it.

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 (see later) in respect of:

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

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,
- persons suspected of committing offences.

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, West Midlands Police has adopted a number of safeguards to firstly avoid this where possible and to then follow a number of arrangements to anonymise any data.

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.

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 is incapable of operating in 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.

The equipment will be worn by uniformed police officers, and the use will be primarily driven by the incidents and circumstances presented to them

or in anticipation of responding to a reported and unfolding incident, or when exercising a specific police power.

General Operating Procedures

Officers will generally receive one of these devices at the start of the period of duty; the equipment is issued on personal basis. A set of operational protocols issued by the wider police service, complemented by the instructions from the respective device manufacturer will be complied with, which ensures the device is charged and all previously captured images and audio is removed. The device will then be fixed to the officer's uniform.

During the course of their normal patrol, the device remains in an inert state and therefore is not recording any material. In order to do so, requires the officer 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 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.
- Officers will also be wearing a badge to visually present the above information.

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 and that their actions and sounds are being recorded. Announcements should be made using straightforward language 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 demonstrate to any subsequent viewer that the incident has concluded and that the user has resumed other duties or activities. 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 custody centre, where other video recording systems are able to take over the recording.

At the end of period of duty, the officer returns the device to his/her station and again, and following a clearly defined process which, in effect involves the officer 'checking in' the device, they 'dock' it into a dedicated port and this automatically downloads all captured information on to a standalone computer. 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.

Once completed, the content on the device are erased and is ready for use again. All information captured and downloaded will be retained on a computer. Any material required to support an on-going investigation or prosecution will be retained as fulfilling a 'policing purpose', and 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). All other material will be automatically erased after 30 days. Access to recordings will be controlled and only persons having an operational need to view specific incidents may view do so.

Where information is captured for use in any investigation, once downloaded on to a computer, 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.

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**.

In order that BWV evidence is admissible in court, West Midlands Police 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**.

The law surrounding BWV

The use by the police of BWV must be shown to be proportionate, legitimate, necessary and justifiable. 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 how West Midlands Police will ensure that the rights and privacy of the public are balanced against the law.

Legality under Common Law

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*)[2]

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*)[3]. (*Murray v the UK (1995)*[4]

Human Rights Act 1998

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' [5]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.

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

[2] R (Diedrick) v Chief Constable of Hampshire [2012] EWHC 2144 (admin) at [9].
[3] R (on the application of Wood) v Commissioner of Police for the Metropolis [2009] EWCA Civ 414 at [98]
[4] Murray v UK (1995) 19 EHRR 193
[5] Ben Jaffey QC December 2013

- 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.

The use of BWV must comply with the 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.

  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 West Midlands Police deploys this equipment, in both the public and private arenas, and then how it deals 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.

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 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 retained where there is no clear evidence of an offence, unless some other good reason exists for their retention.

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])[6]. Recorded conversations between members of the public should always be considered private.

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

West Midlands Police has imposed stricter guidelines where BWV is being used in places not open to the public or where a person being recorded would have a strong expectation of privacy. These include:

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.

Expectation of Privacy

Individuals are likely to have a strong expectation of privacy, in places not generally open to the public, such as a private residence especially at a time of day when people are likely to be in bed. Clear justification of the necessity to use BWV will be required in such circumstances. Furthermore circumstances may dictate an expectation of privacy, even when an incident has occurred in a public area, such as where someone may be the subject of an accident in the street.

Likely to cause serious offence

[6] Peck v United Kingdom (2003) 36 EHRR 41; [2003] EMLR 28

Care should be exercised in using BWV where it may cause serious offence, for example during a religious ceremony.

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.

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.

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.

West Midlands Police will continue to monitor all use of this equipment to ensure that it remains proportionate and undertakes to update this PIA process if their findings warrant any change.

Data Protection Act 1998

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;

Principle 1 of the DPA (fair and lawful processing) requires that the data subject must be informed of:

1. The identity of the data controller
2. The purpose or purposes for which the material is intended to be processed and
3. Any further information that is necessary for processing to be fair

West Midlands Police has the responsibility for controlling this information and is known as the Data Controller for information captured and used within its area, for a policing purpose. If required, a police officer 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. However, West Midlands Police has provided badges to officers to indicate that their equipment captures both audio and video information. Therefore, as a general rule, where an officer is in uniform and is clearly carrying or wearing a suitably identified camera (with labelling as an audio and visual recording device) this condition would be considered to have been satisfied.

In order for West Midlands Police to ensure compliance with the DPA, the following has been undertaken:

- a local media campaign to advertise the use of BWV, using local newspapers and other media and the force website as well as web chats both internally and externally;
- advise the local community-based forums of the use of this technology in the area;
- ensure users where possible/practicable, announce to the subject(s) of an encounter that video and audio recording is taking place using BWV.

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.

For further information relating to the DPA see **ACPO (2013) Data Protection Manual of Guidance v5.2, Part I Standards** and the website of the ICO at www.ico.gov.uk. In addition please see **College of Policing (2013) APP on Information Management**.

Criminal Procedure and Investigations Act 1996

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

West Midlands Police is 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.

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.

Freedom of Information Act 2000

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.

Protection of Freedoms Act 2012 & the Surveillance Camera Code of Practice

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.

West Midlands Police adheres 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.

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

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.

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.[7] 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.

The guidance further states that a Policing Purpose includes:

a Protecting life and property

b Preserving Order

c Preventing the commission of offences

d Bringing offenders to justice

e Any duty or responsibility of the police arising from common law or statute

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

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.

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

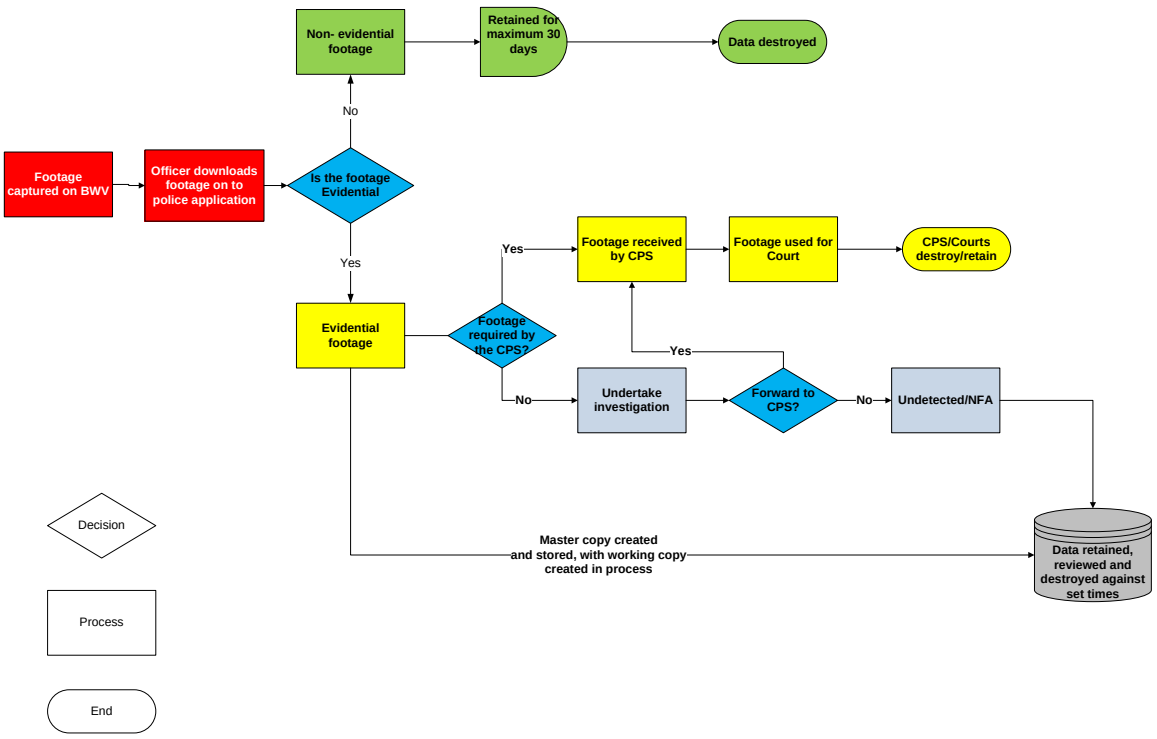
Data Flows

The chart below demonstrates, in simple terms, how information captured on a BWV device is captured, processed and then disposed of. West Midlands Police has the responsibility for the processing of information in its possession which commences at the point when an officer captures it.

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

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.

Where information is shared with the CPS, West Midlands Police no longer has the responsibility for the shared data and the retention timeframes and disposal requirements then revert to that organisation.



Public Acceptability

West Midlands Police sees 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. Since this is a trial of Body Worn Video, there is on-going research to assess the benefits to the public and Police.

- Independent Advisory Panel – February 2014
- PCC Consultation and Public Meetings, March and April
- Birmingham South and West Midlands Police Facebook
- Birmingham South and West Midlands Police Twitter
- Questionnaire – Officers and members of the public (June to December)
- Webchat – Internal and external – June 2014

The current review of data relating to deployments and the questionnaires is on-going with Cambridge University and any results will be used to inform future deployments.

The key messages and issues arising from early consultation are:

- Privacy of data
- Recording capabilities of equipment
- Security of equipment

As a consequence, West Midlands Police considered these against its Privacy Impact assessment and noted these findings in the Privacy Risk Mitigation section.

There will be a repeat of this programme in December 2014.

In the intervening period, West Midlands Police will continue to assess any issues or concerns being brought to its attention or 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 its operational deployment policies.

Privacy Issues and Risk Mitigation

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 West Midlands Police. The purpose of this section is to firstly identify what these issues are and to then provide an explanation of the mitigation West Midlands Police 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 West Midlands Police. However, the force 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 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. Any sharing of the information outside these parameters is generally not permitted.
How will any information be shared with the Crown Prosecution Service,	Any captured information deemed to be evidential, will in the first instance be 'protected' by means of a Master copy being

Defence and the Courts?	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?	West Midlands Police will only deploy this technology against the defined operational requirements and to 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) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier.
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 requirement imposed on its use, and West Midlands Police is 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 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.
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. 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. West Midlands Police adopts a process whereby the devices are booked in and out and the start of an officer's duty. Accordingly, the impact in terms of any time lost between any

	actual loss and notification to the force, 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. West Midlands Police will also notify the Information Commissioner's Office at the earliest opportunity. In addition, in many instances, the captured information is 'stored' on the device's internal memory and to access this requires a bespoke 'docking' facility, which is not widely available. Both the device and the data link between the device and the docking facility are encrypted so it is highly unlikely that any data would get into the hands of a 3rd party.
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 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.
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 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; and • 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. 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 a police officer is present at an incident in a private dwelling and is there for 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 police officer 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. West Midlands Police is very mindful of the concerns that this raises and has trained its users to respect and adhere to these safeguards.

Appendices

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.

Glossary of terms

ACPO – Association of Chief Police Officers

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

PACE – Police and Criminal Evidence Act 1984

PIA – Privacy Impact Assessment

PNB - Pocket Notebook

References and legislation

The Information Commissioner's Office *Conducting Privacy Impact Assessments code of practice*

http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.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://www.acpo.police.uk/documents/crime/2011/20111014%20CBA%20practice_advice_police_use_digital_images_18x01x071.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