# BODY WORN VIDEO PRIVACY IMPACT ASSESSMENT

A detailed assessment of the implications, considerations and aspects of deploying with Body Worn Video technology for parking enforcement.

**Traffic Management & Control Team**

The Highland Council | Roads & Community Works

HQ | Block A 2nd Floor | Glenurquhart Road | Inverness | IV3 5NX

## Table of Contents



VERSIONS

| Date | Revision | Action completed and page reference | Action by |
|---|---|---|---|
| 01/10/16 | 0.1 | Creation of the current PIA | Shane Manning |
| 16/01/16 | 0.2 | Updated, various | Shane Manning |
| 01/02/17 | 0.3 | Revision | Miles Watters |
| 30/03/17 | 0.9 | Draft for Board approval | Shane Manning |
| 01/04/17 | 1.0 | Public Issue | Shane Manning |

## INTRODUCTION

The Highland Council has utilised equipment and completed trials on cameras that are capable of capturing both video and audio information and are known as Body Worn Video (BWV). These have been used by uniformed staff and have been fitted to their clothing. With the progression of technology, the devices have become smaller, lighter, and more easily carried by staff, which has extended their scope of use. It is widely known that members of the public, going about their daily lives, are likely to have their movements and identity captured on a multitude of surveillance systems and it is of paramount importance to mitigate any privacy risks and issues associated with BWV.

## PURPOSE OF PRIVACY IMPACT ASSESSMENT (PIA)

Any new initiative or process that involves gathering, storing or exchanging (processing) of personal data has the potential to give rise to privacy concerns, from the public. Carrying out a PIA is a method of ensuring that privacy issues are minimised and that public concerns for the use of this established technology are alleviated.

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

- the rationale for the Council introducing and using this technology.
- the legality behind its use.
- the likely operational circumstances when staff may use it.
- how the Council will mitigate privacy issues and risks
- how the council will monitor the use of the equipment

The Council will review this PIA in light of ongoing consultation with its community, in response to any national and legislative changes and best practice guidance from the relevant organisations.

## WHAT IS MEANT BY PRIVACY?

The Information Commissioner's Office *Conducting Privacy Impact Assessments code of practice* 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 capturing of a person's home or personal possessions, 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 the Council to anticipate and address the likely privacy impacts of service delivery, in order that problems can be foreseen and solutions developed to ensure that concerns are addressed appropriately.

The Council has established the need for the use of cameras that are capable of capturing both moving images and audio information which are worn by staff both uniformed and, on rare occasions, non-uniformed. The devices will be used for the purpose of parking enforcement and the aim of undertaking this PIA is to:

- explain the extent of their use
- explain their limitations
- describe how any data captured will be processed
- analyse the risks to privacy of the introduction of BWV with reference to the Data Protection principles.

*This PIA relates to the **overt** use of this BWV equipment in relation to parking enforcement. Further use of BWV will require separate PIAs to be carried out.*

## WHAT IS BODY WORN VIDEO (BWV)?

Any style of camera which is carried or fixed to the clothing of a Council officer and is capable of capturing both video and audio information falls under the category of Body Worn Video.

The equipment has been available for a number of years but with advancing technology, the devices have become smaller, lighter, more easily carried by staff 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.

These devices will be mounted on staff clothing while they carry out Parking Enforcement in public spaces. The term staff refers to any person employed directly or under contract by the Council.

## WHY USE BWV?

The Council has a responsibility to enforce Legislation in relation to parking in the public space. This involves stopping or being stopped by and speaking to the members of the public and recording information in their pocket books or handheld devices.

In some instances, the detail of what has been recorded by traditional methods has been the subject of interpretation and the subject of challenge or complaint. Equally it may not have presented the best possible primary evidence to support Council officer's actions and conduct.

BWV devices are able to record exactly what happened, what was said and when, in an indisputable format. Their use will be covered by the management processes described in this PIA and staff will receive training and guidance in their use. The use of BWV by staff must be

- Incident specific
- Proportionate
- Legitimate
- Necessary

- Justifiable

Staff have traditionally used pocket books or handheld devices 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 a pocket book or handheld device and is not a replacement for it.

This equipment may, therefore, be used to record video and audio information of encounters between Council staff 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 crime
- reduction in incidences of public disorder
- presentation of evidence to Police Scotland to bring successful prosecutions before the courts
- transparency of Council practices.
- resolution of complaints

Based on the above, the following categories of members of the public are likely to have their contact with Council staff recorded:

- witnesses of lawful activities
- witnesses of crimes, or those who witness other parties verbally abusing Council staff as they discharge their duties
- witnesses of those who interfere with Council assets including signs and notices
- persons suspected of committing offences

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

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

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

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

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

The Council has reviewed section 7.2 of the Information Commissioner's CCTV Code of Practice which relates directly to BWV when carrying out this PIA and drawing up its guidance for staff:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Other relevant documents include:

The College of Policing BWV guidance
http://library.college.police.uk/docs/college-of-policing/Body-worn-video-guidance-2014.pdf and

The Home Office Guidance for safeguarding BWV data
https://www.gov.uk/government/publications/safeguarding-body-worn-video-bwv-data

## GENERAL OPERATING PROCEDURES

Staff approved to use BWV will 'book out' their BWV device from a pool of devices shared amongst a number of staff. This booking out process, along with their other equipment, is supervised and recorded. This will ensure that a specific device is allocated to a specific member of staff. A specific secure back office BWV computer is used to maintain the integrity and continuity of the device and captured BWV video data. A set of operational guidance notes (appendix 1) has been issued by the Council, complemented by training on the correct use of the BWV device and associated back-office software. Local managers are required to ensure that the device is charged and all previously captured images and audio is removed prior to redeployment. The device will then be fixed to the staff member's uniform.

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

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

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

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

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

The recording is also likely to continue for a short period after the incident to clearly

demonstrate to any subsequent viewer that the situation has concluded and that the user has resumed other duties or activities.

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

- the date, time and location;
- the reason for concluding the recording.

At the end of period of duty, the officer returns the device to their operational base. They must then follow a clearly defined process which involves 'checking in' the BWV device. Their manager, supervisor or team leader 'dock' it into a dedicated port and this automatically downloads all captured information on to a networked computer. This information cannot be deleted or altered. The staff member will then identify the elements of any applicable captured data that is immediately known and needs to be retained to assist in an investigation or review, and 'mark' the section appropriately, by using the built in software.

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

All information captured and downloaded will be retained on a secure drive. Any material required to support potential criminal investigation or prosecution will be retained until passed to the Police via the agreed secure transfer method.

- The secure transfer method involves the copying of the footage both master and working copy onto a disc. This is signed for by means of a Scottish Police Authourity evidence release form and passes into the data control protocol of Police Scotland.
- The original digital copy of the footage is held until the outcome of Police Scotland actions or 2 years whichever is longer.

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

All other material will be automatically erased after 30 days.

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

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

The Council will on occasion share Video recordings with Police Scotland based on Police Scotland evidence recovery protocols. This sharing of information is covered by section 29 of the DPA. Where appropriate, the Police may choose to use the footage to conduct a media campaigned where this is felt appropriate in the detection of crime.

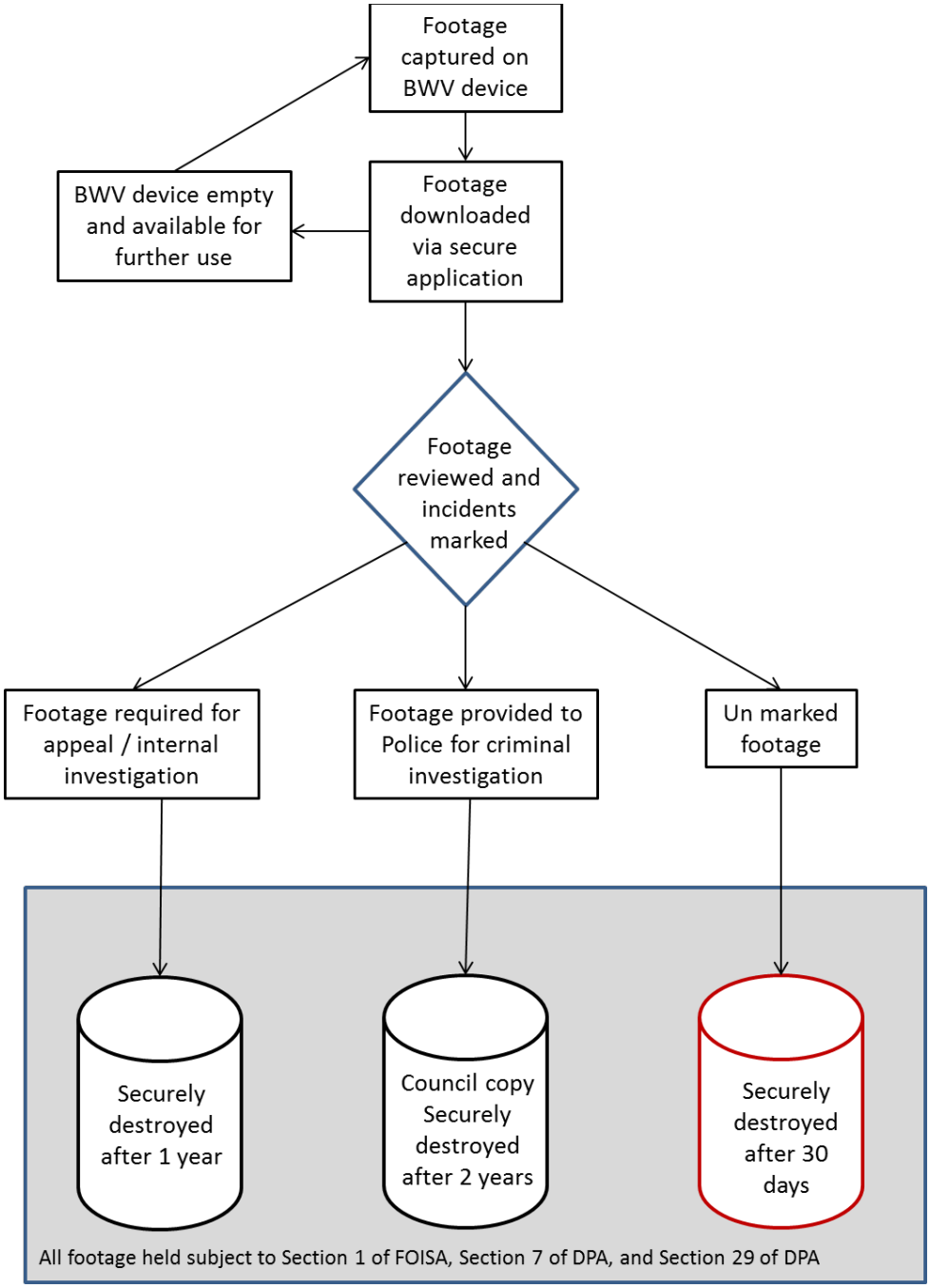
Throughout the time that any data is retained, the Council will ensure that it complies with requests for information under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004. However, it is likely that much of the

information will be exempt/excepted under the personal data exemption/exception.

The Council will also ensure that data subjects (those whose personal data is captured by the BWV device) are able to access the relevant recordings under Section 7 of the Data Protection Act 1998, unless an exemption applies.

## DATA FLOWS

The chart below illustrates the processes described above and indicates the retention periods for the different categories of footage.



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

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

## PUBLIC CONSULTATION

The Highland Council advertised their proposal to use BWV for Parking Enforcement by means of a Notice in the press, online on the Council website and via social media.

After a period of 21 days, only six written responses were received from Highland residents all were positive responses to their use.

The Highland Council will continue to publicise the use of this equipment to ensure that the Public are fully informed of their use.

## EUROPEAN CONVENTION OF HUMAN RIGHTS ACT 1998 (ECHR)

The use of BWV must comply with the all the Articles of the ECHR, 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. This is a qualified right and the Council is required to consider Article 8 when dealing with recorded images, whether they are made in public or private areas.

Accordingly, this PIA has addressed the issues raised by Article 8 and the Council has introduced suitable safeguards for the deployment of BWV and the management of the footage collected.

The principle objective is to ensure that any interference with the rights of individuals can be justified because it is:

- Necessary
- In pursuit of a legitimate aim – such as the prevention, investigation and detection of crime
- In accordance with the law

The Council's justification for using BWV is provided on Pages 4 and 5 above.

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 Council acts with integrity and transparency and potentially provides objective evidence of controversial events. It offers protection for both citizens and the Council.

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.

## DATA PROTECTION ACT 1998

The intention of carrying out a PIA is to ensure compliance with the Data Protection Act 1998 (DPA). This section describes how the Council's use of BWV will comply with each of the Data Protection principles.

**Principle 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.

The purpose of the use of BWV in parking enforcement is to capture higher quality evidence to:

- assist Council Staff in carrying out their legal duties in relation to the Road Traffic (Scotland) Act 1991
- enable action to be taken in relation to specific incidents
- enable the Council to deal with complaints
- protect staff as required by the Health and Safety at Work etc. Act 1974 (as amended) while they carry out their duties by acting as a deterrent

The Council, therefore, believes that the processing is necessary for the compliance with the above legal obligations and that condition 3 of Schedule 2 applies. In the case of sensitive personal data, condition 7(b) of Schedule 3 applies.

**Principle 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.

The purposes for which information gathered using BWV will be used are clearly described in this document.

The Council has carried out a consultation exercise to make the public aware of the plans to use these devices and has publicised their use through press releases and through local media articles.

Information on the use of BWV will be published on the Council's CCTV web pages.

**Principle 3**

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

The Council's operating procedures for BWV are intended to minimise the amount of information collected to reduce the privacy impact of their use.

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

The use of BWV is recommended because it will provide an accurate record of incidents to support the Council in carrying out is duties and also in relation to handling complaints and appeals.

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

The Diagram on page 8 provides details of the retention periods which will be applied in different circumstances. Incidents which are not marked for future action will automatically be deleted after 30 days to minimise the unnecessary retention of information. Other retention periods relate to the timescales involved in handling appeals, complaints and subject access requests.

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

The operating procedures described enable data subjects to request copies of their personal data under section 7 of DPA

It will also be possible to comply with requests made under section 10 of DPA.

The process does not involve automatic decision making or the use of the information held for marketing purposes.

**Principle 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.

The operating procedures ensure that information is downloaded from BWV devices at the end of each shift. The information is then stored in an encrypted format until its secure destruction. Only a limited number of staff have access to the footage during its retention.

The greatest security risk exists when the device in use by operatives in the field. However, the information on the device is also in an encrypted format which can only be read by the proprietary software.

**Principle 8**

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

There is no intention to transfer footage recorded on BWV out with the EEA.

Pictures of BWV cameras of the type that may be used by the Highland Council.



## Appendix 1 - Operational guidance notes

**Staff Operating Procedure for the Use of Body Warn Video**

- Staff will recover a camera unit from the equipment room at the start of your shift.
- Each camera is allocated to an individual officer.
- The camera must bear your Officer Number and Photograph

Note: Under no circumstances should a camera be in the possession of an Officer out with your operating hours.

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

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

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

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

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

The recording is also likely to continue for a short period after the incident to clearly demonstrate to any subsequent viewer that the situation has concluded and that the user has resumed other duties or activities.

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

- **The date, time and location;**
- **The reason for concluding the recording.**

1. At the end of a period of duty, you will return the device to base.
2. Return the BWV device to its cradle.
3. You will inform your supervisor if there is any content requiring review.

**Camera Usage guidelines**

Body Worn Video (BWV) may be used to record video and audio information of encounters between Council staff and the public, after ensuring appropriate safeguards in respect of the necessity, legitimacy and legality are addressed in respect of the following:

- prevention and detection of crime
- reduction in incidences of public disorder
- presentation of evidence to Police Scotland to bring successful prosecutions before the courts
- transparency of Council practices.
- resolution of complaints
- assist Council Staff in carrying out their legal duties in relation to the Road Traffic (Scotland) Act 1991
- enable action to be taken in relation to specific incidents
- enable the Council to deal with complaints
- protect staff as required by the Health and Safety at Work etc. Act 1974 (as amended) while they carry out their duties by acting as a deterrent

Based on the above, the following categories of members of the public are likely to have their contact with Council staff recorded:

- witnesses of lawful activities
- witnesses of crimes, or those who witness other parties verbally abusing Council staff as they discharge their duties
- witnesses of those who interfere with Council assets including signs and notices
- persons suspected of committing offences or contraventions

In addition, persons, unrelated to any specific interaction between Council staff and any of the categories of persons above, might find their activities captured on a BWV device.
**Staff should make every effort to avoid extraneous capture of unrelated persons in video footage.**

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

## Appendix 2 – Frequently asked questions

**Body Worn Video - Privacy Issues & Risk Mitigation**
**Frequently asked questions**

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

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

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

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

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

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

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

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

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

*In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence). Information will only be captured and processed to achieve a legitimate aim as detailed above.*

5) Will the handling of any data change significantly to be of concern?

*The main difference between current sources of information used by the Council (e.g. CCTV) is that BWV captures both audio and video data. Therefore, a principle issue is that without the introduction and adherence to essential safeguards, there is the greater risk of intrusions into the privacy of citizens. However there are appropriate policies and legislative requirement imposed on its use, and the Council is confident that these will minimise this risk.*

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

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

7) What are the safeguards for minimising the retention times for data?

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

*Other data within the evidential category will be retained in order to satisfy the requirements of legislation, the court process if applicable and depending on the type of offence retained, reviewed and disposed of, in accordance with timeframes within the Home Office/NCPE (2005) Code of Practice on the Management of Police Information (MOPi). Any onward retention by the Police will be in compliance with their policies. The Council's BWV database will be linked to the process relating to the control of documents and records allowing for deletion of BWV data in full compliance with the Council's retention policies.*

8) What are the procedures for dealing with the loss of any BWV devices?

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

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

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

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

10) Collateral intrusion is a significant risk, how will this be handled?

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

11) Do you need consent to record an individual?

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

- *Any non-evidential material is only retained for a maximum of 30 days*
- *This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law; and*

- *Recorded material can be accessed on request in writing in accordance with the DPA 1998, unless an exemption applies.*

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

12) Are you allowed to record in private dwellings?

*The process of parking enforcement takes place in public spaces and is unlikely to require Council staff to record information in private dwellings. The issue of collateral intrusion has been discussed above and the Council has taken reasonable steps to reduce the impact that such intrusion could cause.*