



STAFFORDSHIRE
POLICE

Data Protection Impact Assessment

"BWV"

Stage 1

A Data Protection Impact Assessment (DPIA) is a mandatory requirement under the Data Protection Act (2018). Publication improves transparency and can increase the public's understanding of how their information is used.

The Stage 1 DPIA identifies the high level criteria that identify if further risk analysis is required.

The Project manager and Information Asset Owner will complete the stage 1 document and send to the Deputy Data Protection Officer (DDPO)

A decision will be made (after consultation with the Information Security Officer and / or the Data Protection Officer in the event of any ambiguity) on whether the Stage 2 DPIA has to be completed.

This Stage 1 DPIA should be completed at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into the project plan.

Should you have any queries in relation to the Data Protection Impact Assessment Process then please contact the Deputy Data Protection Officer at SPDPO@staffordshire.police.uk

OFFICIAL-SENSITIVE
(Update when complete)

Version	Version date	Requester of change	Summary of change(s)
0.1	20/09/19		
0.2	23/09/19		Changes suggested to evidence.com process
0.3	04/10/19		Data Protection amendments, suggestions and queries
V1.0	30/11/2023	Sgt	Introduction of enhanced features of BWV cameras for a trial

DOCUMENT REFERENCES

Ref	Document Name	Version Number
	BWV and evidence Trail	V1.0

OFFICIAL-SENSITIVE
(Update when complete)

DDPO Assessment

*****DDPO Use Only*****

A. DPIA part 2 is not mandatory.	☐	
B. DPIA part 2 is not required as long as the remedial action listed is carried out. If the remedial action is not carried out, a DPIA Part 2 will be required.	☐	
C. DPIA Part 2 is mandatory.	☐	
Publication Scheme		
Can this DPIA be uploaded to the Publication Scheme, if not give reasons why i.e. sensitive material included that could disrupt policing operations	☐	

Data Protection Impact Assessment (DPIA) Part 1

Please provide as much detail as possible, avoiding technical language and acronyms, explaining the proposal in a way that someone with no prior knowledge could easily understand.

Section 1 - Governance

Project Proposal Name:	BWV T
Information Asset Owner:	
Project Manager/Lead:	SGT
DPIA Coordinator:	
Date on which processing will commence:	1/1/24
Date submitted to DDPO:	1/12/23

Note: DDPO will give an **initial response** within 10 working days of receiving the completed form.

Section 2 - Purpose, Scope and Context

OFFICIAL-SENSITIVE
(Update when complete)

In this section you must explain what the processing is, who it will involve, and the intended impact. You must also demonstrate why the processing is necessary and proportionate, providing evidence to support your assessment.

- The processing must be **necessary** for the specific objective of the proposal.
- It must also be **proportionate**, meaning that the advantages resulting from the processing should not be outweighed by the disadvantages to individuals.

2.1 Please briefly explain the specific aim and purpose of the proposal in a way that someone with no prior knowledge could easily understand; avoid technical language and acronyms.

The Body worn video project has been ongoing for a number of years and there is already in place a Force policy on the use of Body worn video.

The objectives were identified as being

- To Increase officer safety
- To increase public safety
- To bring an increased level of successful prosecutions
- To increase public confidence

The initial project envisaged delivering a force wide single product across Local Policing and Local Neighbourhood Officers, PCSOs and Special Officers, with 1564 cameras across the county. It delivered axon personal issue body cameras and installed a new Digital Evidence Management system, evidence.com

It has indirect links into Mobile Data and Digital Interview recording and is part of the Mobile Data Project Board for governance purposes.

The information being processed by this system is recorded video (and audio) footage, captured overtly by uniformed officers in the course of their duties in circumstances where they consider it is appropriate, lawful and proportionate, in accordance with the policy. The equipment is designed to give clear indication that it is recording.

The video footage may be used for evidential purposes:

- To establish facts or events to inform decisions about a prosecution or alternative out of court disposal
- As evidence in criminal courts or other judicial processes (eg Coroner's Court)
- In the case of an investigation into complaints against the police or misconduct matters.

The filming of members of the public and the retention of this information is subject to Police and Criminal Evidence Act (PACE), Criminal Investigations & Procedures Act (CIPA) and the Data Protection Act.

The BWV trial is aiming to test the new functions of the axon body camera 3/ 4. The new functions of the camera are Live view, GPS mapping, auto alerts.

LIVE VIEW: this allow any person authorised to access a live feed from the camera, enabling the user to see and hear. There is an audit trail to the action and the procedure has been written to ensure the camera operator is informed their camera is being monitored. The camera will also flash purple and give a message on the screen. The Live view is only available when the camera is in record mode.

GPS mapping: the camera is display in the axon evidence.com where the camera is mapping when the camera is in standby mode or record mode. If the camera is in record mode the system will map where the camera was tracking during this time.

Auto alerts: the camera will send an alert to evidence.com if a taser is activated or discharged.

2.2 What categories of personal data will be processed? Provide an overview of the categories of personal data that will be processed, for example: names, DOBs, addresses, health data, criminal records, or any other unique identifiers such as IP addresses, usernames, e-mail addresses.

This is will be the same details currently recorded with the BWV cameras however it will been seen live.

The main difference is the officer locations I will be visible on the maps.

2.3 Will special category data be used in the proposal? (Select all that apply)

- | | |
|--|---|
| ☐ Race | ☐ Trade union membership |
| ☐ Ethnic origin | ☐ Genetic Data |
| ☐ Political opinions | ☐ Biometric Data |
| ☐ Sex life | ☐ Sexual orientation |
| ☐ Religion | ☐ Health |
| ☐ Philosophical beliefs | ☐ None |

2.4 How will the data be collected? Briefly outline how you will obtain the data, examples include: directly from data subjects, from another data set already in the Staffordshire Police's possession, from a different force.

Personal data (Moving and still body worn video camera image and audio data) is obtained utilising a personal issue AXON Video and audio device in the course of a police officer's day to day role. The use of the devices is in line with the terms of use contained within the Staffordshire Police Body Worn Video Policy. (Appendix 1)

OFFICIAL-SENSITIVE

(Update when complete)

The recorded data will be uploaded to evidence.com, a management system that acts as the data processor on behalf of Staffordshire Police (as data controller) in accordance with the data protection Act 2018. The specific process is described below.

During the course of normal patrol, the BWV device will remain in an inert state and will therefore not record any material. To do so, it requires the officer to deliberately activate the device to a record mode (Double press of centre of device to turn on/ Press and hold to turn off) and where practicable, make a verbal announcement to indicate that the BWV equipment has been activated. If the recording commences prior to 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.

At the end of period of duty, the officer will return their issued device and dock it into a dedicated port, this will allow an automatic upload of all captured video onto the evidence.com system. The data cannot be deleted or altered by the officer at any time. Once completed the data on the camera is erased and ready for use again.

Officers are able to access evidence.com through a licence based account which is password protected. They should then locate the footage and categorise it as evidential, failure to mark as evidential results in the automatic permanent deletion of the footage after 31 days. There is also a 'non evidential' category that also ensures, when marked, that the footage is disposed of after 31 days.

Footage that is marked as evidential will then allow further input in relation to type of incident, these types will then determine the length of time footage is kept as per national guidelines under Management of police information

Officers allocated with body worn video devices are on the whole standard users on evidence.com. This enables them to search and play files

All levels of user will have the ability to view and playback all active (that is, not deleted) video files, regardless of who originally uploaded. Officers/staff members must be prepared to justify why a certain file was viewed and must only do so for a valid policing purpose.

Further accessibility will be assigned to identified staff within the case management unit, who have the ability to Burn Discs and Export Files to Desktop. This ensures better control of Body worn video data by ensuring that only authorised individuals can create working copies of video files 'off-system' in line with Force policy.

Permanent deletion only refers to the video file itself. **A record of video file metadata is never auto-deleted.** Standard users are restricted from viewing it and metadata entries for deleted videos do not return in standard user search results. Metadata that is retained permanently includes; Recorded Date, (Uploading) Camera ID, (Uploading) User ID, Incident ID, Notes, Access Audit Log.

The Data will be store on Evidence.com under the respond tab. There is a audit trail for access.

OFFICIAL-SENSITIVE

(Update when complete)

2.5 How will the data be used? Briefly describe how the data will be used, recorded, and stored and who it will be shared with.

For officer safety, assessment of risk and understanding at an incident, for evidential reasons, for devolvment of officers.

The nature of personal data obtained on BWV Cameras will be moving video image and audio data.

Unless impractical to do so by reason of the situation, behaviour or condition of those present, a BWV recording will normally begin with a verbal announcement that a recording is taking place and the reason(s) why this is justified.

Thereafter, the specific content of what is recorded will vary dependant on several factors, including:

- 1) Nature of incident or suspected offence(s)
- 2) Which members of the public present in recording and their relationship to the incident (e.g. suspects, witnesses, victims, bystanders)
- 3) Whether other police officers are present in the recording
- 4) Angle/position of BWV camera and/or position of recording officer
- 5) Location of recording

Personal data could contain sensitive details in relation to an incident, namely details concerning a suspect, witness, victim, bystander or their property. This could well include special category data and/or data that, should a breach occur, would create significant risks to a person's fundamental rights and freedoms. This would not necessarily be limited to the rights and freedoms of those directly recorded, dependant on the content.

In line with Force procedure, BWV footage will **not** contain the following personal data:

- 1) Recordings of intimate searches
- 2) Discussions subject to legal privilege

2.6 How many individuals will the processing affect? (Please specify one answer below)

- ☐ Fewer than 100 data subjects
- ☐ 100 to 1000 data subjects
- ☐ 1000 to 5000 data subjects
- ☒ More than 5000 data subjects

2.7 What categories of data subject are involved? (Please select all applicable categories below)

OFFICIAL-SENSITIVE
(Update when complete)

- ☒ Persons suspected of having committed or being about to commit a criminal offence
- ☒ Persons convicted of a criminal offence
- ☒ Persons who are or may be victims of a criminal offence
- ☒ Witnesses or other persons with information about offences
- ☒ Children or vulnerable individuals
- ☒ Staffordshire Police staff (current and former)
- ☐ Other

If other then please provide further details below:

2.8 Will it involve the collection of new information about individuals? Will Staffordshire Police collect data that it has not previously collected or had access to?

- ☒ Yes
- ☐ No

2.9 Data Sharing

Does the processing involve:

Select one option

- | | | |
|--------|---|--|
| 2.10.1 | Data being shared with third parties external to Staffordshire Police or recipients that have not previously had routine access to the information? | ☒ Yes
☐ No |
| 2.10.2 | Transferring data outside the UK but within the EU? | ☐ Yes
☒ No |
| 2.10.3 | Transferring data outside the EU? | ☐ Yes
☒ No |
| 2.10.4 | Storing data using a cloud service provider? | ☒ Yes
☐ No |
| 2.10.5 | Is there an ISA, contract, or other sharing agreement in place with all parties with whom data will be shared? | ☒ Yes – agreements in place
☐ Not yet – agreements required
☐ No – none required |

2.10 Why it is necessary to use personal data to achieve the aim and why can't the aim be achieved by other means?

For example, can the aim be achieved by using less data or different types of data?
Are all categories of data necessary to achieve the aim?

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/ mobile data devices. 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.

OFFICIAL-SENSITIVE
(Update when complete)

With the introduction of BWV Camera technology, the Force is 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
- Justifiable

BWV is capable of capturing primary evidence (therefore, personal data) 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.

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.

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).

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) (Murray v the UK (1995)).

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' 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 there are a number of 'Articles', which protect the rights of citizens. Some of these Articles are absolute whereas others are 'qualified' and any interference with these is limited. 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: the right to respect for private and family life, home and correspondence and;
- Article 6: the right to a fair trial.

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 and;
- In accordance with the law - legal advice has been sought to establish that BWV is in accordance of the law.

All images from BWV have the potential for use in court proceedings whether they provide information that is beneficial to the prosecution or defence. It must be emphasized 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.

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

Furthermore, all BWV use cases as described under s.2(c) are justified in terms of their requirements for processing personal data due to being necessary and proportionate for law enforcement purposes, as defined in the Data Protection Act (2018) as:

‘The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’

GPS mapping is a safety feature ensure we know where the officers are and we can see live what is going on. The ability to see where officer were on the recording will help in the evidence chain.

2.11 Explain how the use of personal data is proportionate to the aim of the proposal. Weigh the advantages of achieving your purpose against disadvantages to data subjects.

A BWV recording will take place under a multitude of different circumstances and in many locations. Typically, a recording will begin, just prior to, or in the early stages of, an incident response. More specific instances where a BWV recoding is likely to be appropriate and proportionate include:

- 1) When a user decides to use statutory powers to stop a motor vehicle in order to engage with one or more of the occupants
- 2) When users attend premises in order to effect an arrest.

- 3) 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.
- 4) 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.
- 5) When a user decides to conduct the search of a person, premises, land, vehicle, vessel or aircraft in accordance with code A Codes of Practice for PACE or any other statutory power.
- 6) When a user believes an interaction presents or is likely to present a risk to the safety of the user or other persons present.
- 7) Where a user is or may be required to exercise the use of force against persons or property.
- 8) Where a user gives a direction to an individual or group under any statutory power.

The relationship to individuals whose data is being processed is dependent on which members of the public are present in the recording and their relationship to the incident/suspected offence (e.g. whether they are suspects, witnesses, victims or bystanders). The extent to which individuals are likely to expect processing of their personal data is in part dependant on this relationship.

Unless impractical to do so by reason of the situation, behaviour or condition of those present, a BWV recording will normally begin with a verbal announcement that a recording is taking place and the reason(s) why this is justified.

Recording will, where practicable, be restricted to those individuals and areas where it is necessary to provide evidence or intelligence relevant to the incident. It is important that, where practicable, collateral intrusion on those not involved in the incident is minimised –when this is not possible, care will be taken to redact footage (i.e. deliberately obscure video and/or audio) in any clips that are produced for evidential purposes that involve persons or personal artefacts that are of no relevance to the event; this will only be carried out by an authorised unit (e.g. the Digital Video Unit).

The above only serves as mitigation against undue processing of personal data when considering onwards distribution and analysis. The original 'master copy' *will never be redacted* and will remain stored and accessible to all levels of user in Evidence.com for as long as required under its relevant MOPI grade.

Recordings (and therefore personal still and moving image and audio data processed) will likely include children and vulnerable adults from time-to-time. Decisions on whether to make redactions (or even terminate recording) based on vulnerability factors will be made on a case-by-case basis.

The extent to which individuals have control over their data is likely to be in part dependant on their relationship to the incident/suspected offence(s).

Under Part 3 of the Data Protection Act (Law Enforcement Processing) data subjects can exercise the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification

4. The right to erasure or restriction of processing
5. The right not to be subject to automated decision- making.

Individuals who wish to exercise these rights in relation to personal data being processed by the DIRs will be able to do so in the usual channels; the Central Disclosure Unit (CDU) will process Subject Access requests, the RRD Department will process record deletion requests and all other queries should be sent to the Force Data Protection Officer in the first instance.

Body Worn Video footage will likely meet the definition of 'material' as per s.23(1) of the Criminal Procedure and Investigations Act 1996 (CPIA) and therefore will be disclosed to the Crown Prosecution Service (CPS if a charging decision (or charging advice) is requested and the relevancy test is met.

In turn, this be will presented at court as evidence if it forms part of the prosecution. If it does not form part of the prosecution, the CPS will provide the defence (and by implication, the suspect) with the schedules of all the unused material and provide them with any material that undermines the case for the prosecution or assists the defence. This is therefore a means by which the suspect will have access to their personal data.

Witnesses, victims and bystanders do not receive a copy of any relevant BWV footage as part of any legislative requirement or Force procedure.

Other than the GPS mapping data we record the information currently the only additional information we will record to the location data. This gives the advantage of enhancing the evidence chain and officer safety. The live view is simply displaying the already recorded data at the time.

The disadvantage is officers locations will be tracked and recorded

Section 3 – Lawful Basis

3.1 Lawful Basis

To process personal data you must have a lawful basis. Please select the one appropriate lawful basis from the drop down list.

Lawful Basis for **Operational Data** (Personal data processed for law enforcement purposes):

Necessary for a law enforcement purpose

Lawful Basis for **Administrative Data** (Personal data processed for non-law enforcement purposes, e.g. for HR or Commercial purposes):

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority

3.2 Further Special Category Lawful Basis

If processing special category data (section 2.3) you must have identified a further lawful condition

Operational Data:

OFFICIAL-SENSITIVE
(Update when complete)

The processing is strictly necessary (please tick to confirm) ☐

AND

One of the following conditions applies (select from the list):

Choose an item.

Administrative Data:

It is necessary for one of the following conditions (select from the list):

Choose an item.

OR

It is in the substantial public interest (tick to confirm) ☐

AND for the following purpose:

Choose an item.

Section 4 – Review, Retention and Disposal

4.1 Does the proposal have a review, retention and disposal process that complies with Staffordshire Police Policy? All records must have an initial retention period set by the owner of the information when first created or received; review and disposal criteria are defined within the Staffordshire Police Retention and Disposal Schedule on the policy database.

☒ Yes

☐ No

Section 5 – ICO: Additional Factors

The Information Commissioner's Office have published a number of factors that present a 'high risk' when processing personal data. Saying yes to one or more of the following may indicate that the processing is high risk and a Stage 2 DPIA is likely to be required.

Does the processing involve:		Please check either Yes or No	If 'Yes' then please provide further details
5.1	Systematic, extensive and large scale profiling and automated decision-making about people? <i>"Any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects, or significantly affect the natural person"</i> Profiling is any form of processing where personal data is used to evaluate certain personal aspects relating to an	☐ Yes ☒ No	

OFFICIAL-SENSITIVE

(Update when complete)

	individual, including the analysis or prediction of an individual's performance. Automated decision-making involves making a decision that affects someone by technological means without human involvement, for example issuing speeding fines solely based on evidence captured from speed cameras.		
5.2	Large scale use of special category data or criminal offence data? <i>"Processing on a large scale of special categories of data, or personal data relating to criminal convictions and offences referred to in Article 10"</i>	☒ Yes ☐ No	
5.3	Public monitoring? <i>"Systematic monitoring of a publicly accessible area on a large scale"</i>	☐ Yes ☒ No	
5.4	New technologies or techniques? <i>"Processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence)"</i>	☒ Yes ☐ No	
5.5	Profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? <i>"Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data"</i>	☐ Yes ☒ No	
5.6	Biometrics/genetic data? <i>"Any processing of biometric data" and/or "any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject" Biometric data can include Facial Recognition technology, fingerprints and is defined as</i>	☒ Yes ☐ No	
5.7	Data matching? <i>"Combining, comparing or matching personal data obtained from multiple sources"</i>	☒ Yes ☐ No	

OFFICIAL-SENSITIVE

(Update when complete)

OFFICIAL-SENSITIVE
(Update when complete)

5.8	Invisible processing? <i>"Processing of personal data that has not been obtained direct from the data subject in circumstances where providing a Privacy Notice would prove impossible or involve disproportionate effort"</i> For example, when gathering data, without the knowledge of the data subject, in the course of a Police investigation.	☒ Yes ☐ No	
5.9	Tracking? <i>"Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment"</i>	☒ Yes ☐ No	
5.10	Targeting of children or other vulnerable individuals? <i>"The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children"</i> For example, the use of personal data relating to children for the purposes of marketing their online safety products.	☒ Yes ☐ No	
5.11	Risk of physical harm? <i>"Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals".</i> For example, if data relating to CSAE, HUMINT or protected persons data was compromised then it could jeopardise the safety of individuals.	☐ Yes ☒ No	
5.12	Evaluation or scoring? <i>"Aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" For example, as part of a recruitment process.</i>	☒ Yes ☐ No	

OFFICIAL-SENSITIVE
(Update when complete)

5.13	Data processed on a large scale. <i>Considerations include:</i> • The number of data subjects concerned • Volume of data and/or range of data items • Duration, or permanence, of the data processing • Geographical extent of data processing	☒ Yes ☐ No	
5.14	Preventing data subjects from exercising a right? <i>The rights are:</i> • The right to be informed • The right to access data • The right to rectification • The right to erasure • The right to restrict processing • The right to object • The right to portability • Rights relating to automated processing	☒ Yes ☐ No	

Please forward the completed form the Staffordshire Police Deputy Data Protection Officer. SPDPO@staffordshire.police.uk.

Summary of Initial DDPO advice:
Additional advice from ISO and or DPO