Decision Note – BWV (Body Worn Video) and DIR (Digital Interview Recording) Contract

STAFFORDSHIRE COMMISSIONER
Police | Fire and Rescue | Crime

REQUEST FOR DECISION BY THE STAFFORDSHIRE COMMISSIONER

	Policing:	Crime:	Fire & Rescue:
This decision relates to:	✔	✔	

APPROVAL (for completion by Staffordshire Commissioner only)

Rationale for approval

STAFFORDSHIRE COMMISSIONER

Signature **Date** **22/12/21**

Date decision required by: 10th December 2021
If an urgent approval is required, please state reasons: This is an urgent request, as the current BWV contract expires at the end of December 2021. Commercial Services have negotiated 2 x 3-month extensions to the BWV contract, whilst internal discussions continue on the provision of DIR

alongside the BWV contract. Due to on-going issues with IT and the IT Plan, this decision has yet to be made as to where and how DIR features within the IT Plan.

As we are now near the end of the second 3-month extension period a decision back to Axon needs to be communicated by close of business on Friday 10th December. There is no further room for negotiation of short-term extensions. Therefore, an urgent decision is required.

For completion by Staffordshire Commissioner's Office only:-

Decision Number: SCP/D/202122/007

Date Received: 22 December 2021

	Yes	No
Has the required decision been considered under the guidance of the Staffordshire Commissioner's Decision Making Policy?	x	
Has the required decision been deemed to be a Key Decision as defined within the Staffordshire Commissioner's Decision Making Policy?	x	
Who is empowered to make the required decision? Staffordshire Commissioner		

Title	Body Worn Video and Digital Interview Recording

The Body Worn Video (BWV) contract is requiring renewal by the end of December 2021. It is proposed that following exploration of options, the existing arrangement with Axon is continued.

Given the need to modernise, the force wishes to upgrade and extending its capability to record interviews digitally, with both video and audio functionality; this is called Digital Interview Recording (DIR). Following a market assessment, the preferred solution is to contract with the same supplier as BWV (Axon) driving a better pricing structure and ensuring a seamless link between products.

The Commissioner is requested to support the BWV renewal and the proposed DIR solution.

Recommendation:

That the Commissioner approves contracting with Axon for the delivery of BWV and DIR functionality within Staffordshire Police

Chief Executive

I hereby approve the recommendation for consideration.

Signature  Date 22/12/21

REPORT AND ADVICE TO THE STAFFORDSHIRE COMMISSIONER

1. Introduction and background

The Body Worn Video (BWV) contract is requiring renewal by the end of December 2021. The work on the new contract has been on-going for a significant amount of time to ensure that the force is receiving best value for money on this.

Several options for BWV have been explored including different licensing arrangements and storage requirements. Based on the approach selected, the proposed BWV as-is renewal for licences and storage (evidence.com) is within the 10% tolerance for the renewal of contracts and can therefore, be progressed.

In line with modern practices, the force is in urgent need of upgrading and extending its capability to record interviews digitally, with both video and audio functionality; this is called Digital Interview Recording (DIR). Therefore, alongside the option to procure the new BWV contract, the force proposes to implement DIR across various sites and procure a mobile functionality as well. Following a market assessment, the preferred solution is to contract with the same supplier as BWV (Axon) driving a better pricing structure and ensuring a seamless link between products.

The Commissioner is requested to support the BWV renewal and the proposed DIR solution.

2. Issues for consideration

The new Axon BWV contract is based on a 7-year deal with a break clause at years 5 and 6.
The Axon DIR contract is for 5 years.

The contract has a fixed pricelist to purchase BWV and DIR hardware and software items for the first 5 years of the contracts. This is the critical point, to allow the best value for money for the force.

A number of assumptions have been made to determine the contract value:

- Current BWV licences and storage requirements over the contract life;
- Projected future volumes for the replacement of BWV hardware over the contract life;
- DIR hardware and licensing for 22 DIR rooms and 4 mobile kits over the next 2 financial years, profiled for an initial 2 test rooms for evaluation (21/22) with a break clause;
- Any amendment to the above will affect the current pricing offer that has been provided.

There are some key benefits of contracting BWV and DIR together;

- A significantly improved price point saving approximately £150k per annum;
- DIR project timeline coincides with the BWV renewal, so is timely and works to the refreshed IT Plan;

- The full tender for DIR was initially conducted by BDUK with market assessment seeing Axon providing the best solution. This gives assurance on value for money against the market offerings.
- The DIR proposal has additional functionality such as Axon Citizen, allowing the public to securely upload video evidence into evidence.com, as well as providing transcription functions turning interview audio into text and further with options to explore analytics and redaction functions.
- The relationship with Axon is embedded following an initial significant investment 5 years ago with BWV. The supplier is a market leader offering solutions to enhance policing which also aligns to the IT plan plans and strategic direction of Staffordshire Police.

There are some risks identified also, but several of these can be managed over the contracted period of time;

- The current DIR kit doesn't meet the needs of the organisation and maintenance of existing kit for extended period will be costly. This is a project risk rather than contract risk;
- Committing budget in advance, although clauses to withdraw off-set this risk;
- Current equipment is end of life and pace is needed to progress, with resourcing needed operationally and technically;
- The timeline to deploy 22 rooms is likely to take a minimum of 12 months which does allow the estates issues and operating model requirements to be addressed.

There is mitigation for these risks and this is to be implemented.

Costs

All costs have been removed as they are commercially sensitive information.

3. What other options have been considered?

There is the option to decline the DIR commercial proposal and just contract award for BWV through Axon. This will however, increase the cost of BWV contract and will in time push the DIR cost up once the DIR replacement is on the IT Plan.

The early preliminary work that Boeing completed on DIR was valuable, comparing options for the future and assured value for money by contracting both DIR and BWV together through Axon.

4. Consultation and Engagement undertaken

Various people have bene involved in the work to date on this contract. IT have been involved for the longer-term planning against the IT plan. This has also been discussed at the Technology, Innovation and Change Board and at the Modern Policing Enabling Board.

Jen Mattinson, T/ACC has also been sighted on the proposals alongside Jason O'Toole, CSupt, to give an operational view and perspective.

Report Implications

Monitoring Officer comments:

The approval requested aligns with the requirements of PFCC / Staffordshire Police delegated powers.

Signature  Date 22/12/21
Section 151 Officer comments: From a contracting point of view, coupled with an operational requirement to move to DIR the financial case for contracting in one makes financial sense. My concerns around this centre around a separate issue of IT delivery of the new Digital Interview Recording project. The Commissioner should note that this project has been in development for a number of years (including when still in contract with BDUK). If this project is not approved (noting it is in the current IT and capital plan without an approved business case) and work started, a risk is present that whilst the overall contract represents VFM this would be at risk unless work on the DIR solution is done at pace. It is unclear as to why this has not been progressed over recent years despite the clear business need. I shall look to ensure that a business case for DIR is brought forward as part of the current MTFS process with a view that work is commenced before the end of the current financial year
Signature  Date 08/12/2021

	Yes	No
Has legal advice (outside of that provided by the Monitoring Officer) been sought on the content of this report?		✔

Legal Comments:

Not required

5. Equality Comments – please attach the completed EIA

Attached

6. Background/supporting paper

None

7. Public access to information

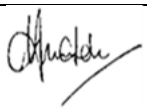
Published on the commissioners website, reported as a decision to Police, Fire and Crime Panel

8. Data Protection Impact Assessment - please attach the completed DIA

Attached
9. Is the publication of this form to be deferred? No
10. If the report is for publication, is redaction required? Redaction of commercially sensitive information is required.

	Yes	**No**
Of the Decision Note?	✔	
Of the Appendix?		**N/A**

ORIGINATING OFFICER DECLARATION:

Author	**Helen Holden,**
Signed	
Date	**8/12/2021**

Equality Impact Assessment

The purpose of this EIA is to ensure you consider any equality issues as part of your decision making when developing / reviewing your policy / procedure.

Please complete the sections below and send to the Staffordshire Commissioner's Office to be quality assured. New / revised policies cannot be published on the policy database until the EIA has passed the quality assurance process.

Title of policy/procedure:	Axon contract to renew the Body Worn Video Services. Contract 3926
Department:	Technology Services
Date:	20/12/2021

1. Identify the aims and purpose of the policy
The contract is for the provision of goods and services for a period of 7 years, with the option to break the contract at 5 years. The services are to maintain licensing and support for the current fleet of Body Worn Video (BWV) Cameras and purchase replacement hardware as required.
2. Identify the individuals and organisations who are likely to have an interest in, or be affected by the policy.
Technology Services – Staffordshire Police Justice Services and Response – Staffordshire Police Operational Staff and Officers – Staffordshire Police

Members of the public

3. Data Summarise the findings of any monitoring data / information which you have considered regarding the impact of this policy on people from all or any of the protected groups. This could include national or local data.
3.1 Age n/a
3.2 Disability n/a
3.3 Race n/a
3.4 Religion or Belief n/a
3.5 Sex n/a
3.6 Sexual Orientation n/a

3.7 Transgender

n/a

4. Research

Summarise the findings of any research you have considered regarding this policy for all or any of the protected groups. This could include information you have obtained from other sources e.g. Home Office.

4.1 Age

n/a

4.2 Disability

n/a

4.3 Race

n/a

4.4 Religion or Belief

n/a

4.5 Sex

n/a

4.6 Sexual Orientation

n/a

4.7 Transgender

n/a

5. Consultation

Summarise the opinions of any consultation for all or any of the protected groups. Who was consulted and how e.g. survey, discussion, forum.
If there was no consultation please justify why.

5.1 Age

n/a

5.2 Disability

n/a

5.3 Race

n/a

5.4 Religion or Belief

n/a

5.5 Sex n/a
5.6 Sexual Orientation n/a
5.7 Transgender n/a

6. Conclusions Taking into account the results of the monitoring, research and consultation, set out how the policy impacts or could impact on people from the following protected groups? (Include positive and/or negative impacts)
6.1 Age n/a
6.2 Disability n/a
6.3 Race n/a

6.4 Religion or Belief n/a
6.5 Sex n/a
6.6 Sexual Orientation n/a
6.7 Transgender n/a

7. Decisions

If the policy will have a negative impact on members of one or more of the protected groups, explain how the policy will change or why it is to continue in the same way.
If no changes are proposed, the policy needs to be objectively justified.

There will be no impact on any of the protected groups by the purchase of these goods and services. The use of the services are controlled by Data Protection Regulations regarding the capture of image and storage of images.

8. Monitoring arrangements

If the policy is new what consideration has been given to piloting the policy?

If monitoring is not already in place what arrangements have been made to monitor the effects of the policy on equality and diversity?

n/a

This equality impact assessment will be published on the SC website.

EIA Form Dated
01/08/2018

STAFFORDSHIRE POLICE

Data Protection Impact Assessment for

Body Worn Video update

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

The DPIA guidance should be read in conjunction with the completion of this DPIA.

Upon completion of the DPIA template the Project Manager and IAO will review, sign off and send a copy to the Deputy Data Protection Officer. The Deputy Data Protection Officer will review and seek the views and approval of the Information Security Officer. The DPIA will then be considered by the Chief Information Officer/Data Protection Officer and if agreed signed off by the Senior Information Risk Officer (SIRO). The SIRO may at this point ask that additional work is carried out or may decline the proposal and not accept any risks identified.

If the DPIA identifies a high risk and measures cannot be undertaken to reduce the risk then there is a requirement for the Force to consult with the Information Commissioner's Office (ICO). Consultation with the ICO will be undertaken by the Information Governance and Assurance Department.

This DPIA should be filled out 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 Information Governance and Assurance Department.

DOCUMENT CONTROL

System Owner	Business Lead	Information Asset Owner	Project Manager
	DCC Baker	C/Supt Tweats	

Author	Role	Department
Robert Neeson	FIM	Contact & Response
Contributors	**Role**	**Department**
Stephanie Ough	JSSU Supervisor	JSSU

Version	Version date	Requester of change	Summary of change(s)
0.1	20/09/19		
0.2	23/09/19	Stephanie Ough	Changes suggested to evidence.com process
0.3	04/10/19	Diana Litherland	Data Protection amendments, suggestions and queries

DOCUMENT REFERENCES

Ref	Document Name	Version Number

Screening Questionnaire

The following questions are intended to help you decide whether a DPIA is necessary. The DPIA guidance document will assist you during the project lifecycle. Answering 'yes' to any of the following screening questions is an indication that a DPIA is required. You can expand on your answers as the project develops.

If there is no personal data involved then go to Section 8 – Conclusions.

"Personal data" means any information relating to an identified or identifiable living individual - Section 3(2) of the Data Protection Act 2018.

Does the intended processing of personal information involve any of the following?

	Intended processing	**Yes**	**No**
1.	Systematic and extensive profiling with significant effects?		x
2.	Large scale use of sensitive data?		x
3.	Public monitoring?	x	
4.	New technologies (processing involving the use of new technologies, or the novel application of existing technologies (including AI)?		x
5.	Denial of service: 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?		x
6.	Large-scale profiling: any profiling of individuals on a large scale?		x
7.	Biometrics: any processing of biometric data?		x
8.	Genetic data: any processing of genetic data?		x
9	Data matching: combining, comparing or matching personal data obtained from multiple sources.		x
10.	Invisible processing: processing of personal data that has not been obtained direct form the data subject in circumstances where the data controller considers that compliance with Article 14 of the GDPR would prove impossible or involve disproportionate effort.		x
11.	Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.		x
12.	Targeting of children or other vulnerable individuals: the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if there is an intention to offer online services directly to children.		x
13.	Risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of individuals.		x
14.	Any other processing which is large scale involves profiling or monitoring, decides on access to services or opportunities or involves sensitive data or vulnerable individuals.		x

Step 1 – Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
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 2200 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.

Step 2 – Describe the processing

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

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

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

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include

children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
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 video) 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.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

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.

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.'

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The use of and collection of information from Body Worn Video is monitored through the Digital policing board for governance purposes.

There is also a newly instigated Body worn video working group.

Use of Body worn video also forms part of a monitoring and consultation process undertaken by the police, fire and crime commissioner's office. There is a particular focus around use of stop search, use of force and use of Taser. These are regularly monitored and fed back through locally based Safer Neighbourhood Panels.

Further scrutiny was presented to the public through the documentary series Cops UK, Body Cam Squad. This generated focus on the successful use of the project

Step 4 – Assess necessity and proportionality

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

Body worn video devices and Evidence.com will be processing personal data for a Law Enforcement purpose and will be lawful under GDPR EU 2016/679 Article 6 (e), the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
therefore this section has been completed in accordance with Part 3 of the Data Protection Act, 2018.

Principle 1: ~~Use~~ Processing of personal data for any of the law enforcement purposes must be lawful, and fair:

The processing is strictly necessary for the law enforcement purpose,
The processing, dependent on the specific circumstances of each case, will meet one of the conditions specified in Schedule 8 and will lawful under GDPR EU 2016/679 Article 9, 2 (g) the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The following is in place to meet the 'appropriate policy' requirement:

- Force DP Policy
- Force Retention Schedule
- This DPIA
- BWV Policy

Principle 2: The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate and; personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected:

BWV footage will be determined by the officer operating the camera, however there are clear procedures that cover when the camera should and should not be utilised. It would be disproportionate for a BWV to be recording for an entire shift.

BWV footage will not be used for any secondary purpose that is incompatible with the original reason it was collected.

Principle 3: data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed:

BWV will only record a specific incident where the officer operating the camera determines that it is proportionate and necessary to do so. The BWV recordings will also be retained in accordance with MoPI.

Principle 4: Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay:

By nature of the data being processed, the records cannot be inaccurate. DIR and BWV will both make an accurate recording of what took place at the time. These records will not be updated or amended in any way.

Principle 5: Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for the law enforcement purposes:

BWV data is only stored on a camera (in an encrypted state) for the duration before it is next docked with an upload station again. Thereafter all content on the camera is erased and the camera ready for use again.

Once uploaded onto Evidence.com, non-evidential video data is retained for 31 days.

Principle 6: Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and accidental loss, destruction or damage:

All Staffordshire Police personnel that are users of the BWV devices are mandated to complete the mandatory NCALT Data Protection Package and MOPI Packages which will ensure that they understand their obligations in handling this data appropriately. They will also have access to the force Body worn video policy and relevant initial training on BWV/ Evidence.com

All Staffordshire Police personnel that are users of the body worn video devices and evidence.com will have been appropriately vetted as part of their employment or voluntary status within the organisation.

Part 3 of the Data Protection Act 2018 provides individuals with the following rights:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure or restrict processing; and
- The right to not be subject to automated decision making.

Certain rights under the GDPR, such as the right to object and the right to data portability, do not exist in Part 3 of the Act. Further, there are exemptions and restrictions that can, in some circumstances, be legitimately applied to prevent individuals from exercising rights. The subject access rights, rights

to rectification and rights to erasure and restriction do not apply to the processing of 'relevant personal data' in the course of a criminal investigation or criminal proceedings.

Data subjects wanting to exercise their right of access would be entitled to do so by submitting an application via a subject access request.

There will be occasions where footage is required by other organisations or individuals as part of a subject access request. The relevant departments will have the necessary means to share the data electronically or through the burning of a disc in isolated cases.

Data Subjects wanting to exercise any of their other rights, or complain should contact the Force Data Protection Officer.

3 Chapter 5 of the Data Protection Act 2018 addresses personal data transfer to a third country

There are three conditions that must be met before a transfer can be made:

- The transfer has to be necessary for any of the law enforcement purposes
- The transfer has to be based on either a finding of adequacy in respect of the third country, or where other appropriate safeguards are in place, or if not, that the transfer is for certain specified special circumstances
- The transfer is to a relevant authority in the third country, or is a 'relevant international organisation' i.e. and international body that carries out functions for any of the law enforcement purposes.

It may still be possible to transfer personal data to a body which is not a relevant authority if additional safeguards can be met.

~~9.~~ Part 3 Chapter 2 of the Data Protection Act 2018 requires that the force demonstrates how they are complying with the principles and states explicitly that this is the responsibility of the Data Controller

Operational Security and Data Protection will form a standing agenda item at Body worn video working group meetings and at the digital policing board

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. BWV has the potential for privacy intrusion. A perceived infringement of privacy could be challenged at court on a number of grounds, including violation of articles 6 and 8 of ECHR. This could cause the collapse of a trial.	possible	Significant	medium
2. Evidence.com has the capability to export/ burn video files (personal data) which could be shared with external persons/ agencies with limited audit trail.	Possible	Significant	Medium
3. BWV Cameras are lost or stolen during operational deployment, leading to the irretrievable loss of personal data already captured	Possible	Significant	Medium
4. Collateral Intrusion (i.e. personal data processed via BWV Recording of bystanders) could be legally challenged by impacted individuals if discovered. Alternatively, identifying persons impacted by collateral intrusion might be extremely difficult, prohibitively costly, if not impossible, when responding to Subject Access Requests.	Possible	Significant	Medium
5. As footage is uploaded onto evidence.com as 'non-evidential' it requires officer intervention to review and determine if of evidential value. As all non-evidential footage is configured to auto-delete after 31 days there is a risk that important footage of evidential value could be permanently deleted. This could stifle an active investigation and reduce or remove the possibility of a successful prosecution.	Probable	Significant	High
6.			

See the Force Risk Management section on the Intranet for further information regarding risk management.

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
1.	Staffordshire Police recognises the potential concerns from the public regarding privacy issues. The policy states that the use of BWV should 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 (2018) and Human Rights Act 1998 and retained and subsequently disposed of in accordance with the Management of Police Information guidance and codes of practice.	Accepted	Low	Yes/no
2.	Evidential material is shared with the Crown Prosecution Service, Defence professionals and the Courts to support a prosecution. Any sharing of the information outside these parameters is through a Subject access request. Protection against this is enhanced via the inability for standard users to export files to desktop.	Reduced	Low	
3.		Eliminated		

4.	It is not possible to negate the loss or theft of a devise such as in a violent scenario, which may lead to the loss of data. The means to attach the device to uniform reduces but does not ensure loss. The personal issue of devices also gives a clear and auditable track of devices and means the impact in terms of any time lost between any actual loss and notification to the force, is kept to a minimum. The captured information stored on the device 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. It is inevitable that this will occur. Officers are trained to be aware and consider such intrusions and should wherever possible, keep the focus of their activity on the subject of the officer's attention. In circumstances where bystanders are captured in any video or audio information and they are unrelated to any offence under investigation, their identities being protected and anonymized should be considered. Incidental captures of bystanders in response to a subject access request,	Reduced	Low Low	

5.	should be considered excessive and refused. This refusal will need to be logged and reported to the Information Commissioner Automated e mail is sent to officer who owns the footage to ensure that any evidential material is marked appropriately prior to the 31 day deletion point	Reduced	Low	

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
Deputy Data Protection Officer (DDPO) advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DDPO advice:		
DDPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		

Chief Information Officer/Data Protection Officer review/advice:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Step 8 - Conclusions

Please provide a summary of the conclusions that have been reached in relation to this projects overall compliance with the DPA. Includes references to any changes that were introduced as a result of the DPIA process.

Sign-Off Authority	Role	Date	Signature
	Senior Information Asset Owner		
	Information Asset Owner		
	Project Manager		

	Information Security Officer		
	Chief Information Officer/Data Protection Officer		
	Senior Information Risk Owner (SIRO)		