Data Protection Impact Assessment

Body Worn Video Camera (BWV)

April 2025

Project name: Body Worn Video Camera (BWV)

Data controller(s): Boston Borough Council (on behalf of Boston Borough Council, East Lindsey District Council and South Holland District Council) referred as "Councils"

Part 1 - Background

1. **Identify why your deployment of BWV cameras requires a DPIA**:
   - Public monitoring
   - Risk of harm
   - Possible capture of Special category data

This process will involve exchanging personal information, which inevitably gives rise to privacy concerns from the public.

The data collection, sharing and processing will be undertaken within a clear legal framework with minimum intrusion on an individual's privacy.

This Data Protection Impact Assessment (DPIA) will assess privacy risks to individuals as part of the collection, use and disclosure of information, within projects and policies that involve the processing of personal data.

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the UK GDPR)?

This is not a new deployment, but a broadening of the Controller party remit as Councils merge.

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve? Set out the context and purposes of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

In going about their daily routine, the Councils Enforcement Officers routinely suffer verbal abuse and can be subject to complaints from the public due to the nature of the role they perform.

Often in all these situations factual evidence of what took place is confined to one person's word against another. This does not leave The Councils in a satisfactory position and the safety of the public is indisputably put at risk.

The Councils hopes to implement BWV cameras that are capable of capturing both moving images and audio information. They would be worn by specific front line service staff attending calls and following up enquiries etc.

The audio and visual images captured shall be associated with acts of verbal and physical aggression and violence, and captured in accordance with information, instruction and training. It is not intended to capture any sensitive personal data. However, it is recognised that this may occur depending on each individual situation as BWV devices not only record both video and audio but they employ wide lenses that captures a broad field of view. This can result in the capture of much larger amounts of personal information than the user intended.

4. Whose personal data will you be processing, and over what area? Set out the nature and scope of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

These devices are for the safety and security of The Councils Officers and the Public. The BWVs will record the data of all individuals who may be picked up by the audio or visual coverage of the device. They will record when conducting official Councils business in areas such, as but not confined to Environmental Health, Licensing, Illegal disposal of household, industrial or controlled waste and neighbour disputes.
Images of people whether victims, suspected offenders, witnesses, bystanders, or officers will be captured on BWV before stored on secure but accessible storage. The system records anyone within its field of lens view, so may capture images of people and record what they say.

The recorded data subject will be individuals the Councils Officer deems appropriate to record due to the situation they are in at the time. This will usually be members of the public.

The Councils BWV cameras can capture both moving images and audio information. They would be worn by operational front line staff attending calls or making enquiries in both public and private areas making enquiries into potential offences.

The audio and visual images captured shall be associated with acts of verbal and physical aggression and violence, and captured in accordance with information, instruction and training. It is not intended to capture any sensitive personal data. However, it is recognised that this may occur depending on each individual situation as BWV devices not only record both video and

audio but they employ wide lenses that captures a broad field of view. This can result in the capture of much larger amounts of personal information than the user intended.

Collateral intrusion – As above, it is possible however that the camera field of view may include individuals (members of the public, staff, etc.) not directly involved in the incident, i.e. bystanders, resulting in individuals being recorded by devices without them being fully aware. This is known as collateral intrusion and 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 will be trained to ensure that wherever possible, the focus of their activity is on the subject of attention. In circumstances where members of the public 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.

Any requests received under subject access will also be managed in line with data protection requirements as they are entitled to their personal data, but are not entitled to another person's personal data, especially if this could cause harm. It is also recognised that once information is released, it is not possible to restrict or control how the data subject shares the information provided to them. It is recognised that information from a BWV could be posted by the recipient on Social media and may attract views from those not involved in the incident.

To control the amount of Collateral intrusion, the BWV device will only be turned on by the staff member if required due to an escalation in an incident. The incident could happen in many locations e.g., public areas, domestic property, work locations etc. where staff are lawfully carrying out their duties.

Personal information collected along with images of individuals could also include names, address, data of birth, business contact details etc.
Specific examples also could include collecting personal information:

- Visual and verbal identification of staff member by name.
- Private conversations and comments.
- Staff and others in a distressed nature.
- Information displayed on personal mobile phones.
- Other identification data such as financial details.
- Vehicle registrations/make and model of cars or business vehicles.

Private Home

- Details of children whether present or not.
- Domestic order of property.
- Occupants in a state of undress.
- Identification of visitors etc.
- Emotionally distressed occupants.
- Identification of occupants.
- Visible personal health indicators

Council properties

- Details of information concerning investigations.
- Building access codes.
- Building layouts.
- Identification of other staff on premises.
- Security protocols.

Special Category data may include:

- Intrusion of private contemplation.
- Intrusion of private ceremonies.
- Identification of people attending group sessions.
- Religious or philosophical beliefs.

Health details.

- Health data, data concerning a person's sex life or sexual orientation, racial or ethnic origin, political opinion, religious or philosophical belief may be inadvertently captured in the event that a member of the public assaults a member of staff, during treatment it may be the video and audio recording collects levels of this information.

No staff member will be issued a BWV device without having completed the relevant training package.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

Only trained and authorised individuals will sign out and deploy the BWV devices. The Council's Assistant Director for Regulatory Services, CCTV Manager and Data Protection Team will make policy decisions as to how the systems are utilised.

Schedule 2 of the DPA 18 allows Councils to share material with a number of agencies where it is necessary on a case-by-case basis to prevent or detect a crime or apprehend or prosecute offenders.

Due to the nature of the specified purposes, there is likely to be sharing of data with Lincolnshire Police, the Courts, other departments within the Council and similar public organisations. From time to time it may also be shared with the Media during public appeals for information etc.

It may also be necessary to use some of the footage for media purposes, for example for appeals for information or to illustrate the Council's work and successes.

6. How is information collected? (tick multiple options if necessary)

- Body Worn Video Camera
- Contemporaneous notes made either in Pocket Notes Books or witness statements to back up the footage.

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

How do you intend to share the Personal Data / Special Category Data securely? What methods will you use to protect the information in transit? Have you consulted with your IT department?

The device chosen for this programme is used widely by emergency responders and Local Authorities across the UK.

i. The system firstly stores recorded information on the device in an encrypted format. This information can only be decrypted when the camera is docked in a Council approved system docking station and uploaded onto our system.
ii. All information is stored on our own servers, and not the cloud based solution. All access to material saved on Video Manager is digitally recorded and auditable. Our policy only allows access to recorded material to a very small number of staff. All these features ensure that the system more than complies with the Data Protection Act.
iii. The cameras have inbuilt optional functionality, such as Bluetooth, Wi-Fi and linking to accessory sensors, however none of these features have been activated or will be utilised by The Councils.
iv. Only footage uploaded onto The Councils software can be redacted / deleted. The software produces a full audit log of all actions carried out on the software.
v. We have activated the automatic deletion policy. Any information not saved as an incident is automatically deleted after 30 days.
vi. All information stored on the device is encrypted to the highest industry standards.
vii. Users report any faults / defects via a dedicated email address to the IT team.
viii. The Councils recognise the need to ensure evidence is only accessible by authorised users.
ix. Our IT Department and procurement team have chosen a BWV model which allows us to configure a number of security features to control access and activity for each user, for evidential requirements and security of the device. This is based on the context and requirements to retain the footage. The features of the devices ensure the authenticity of

any digital footage while meeting chain of custody requirements to prove the integrity of evidence in court where appropriate.

x. The integrity and confidentiality of the device, enabling continuity along the evidential chain and protecting and managing personal data is further assured by:

a) There is a digital evidence integrity chain of a full audit trail with generated checksums and watermarked evidential outputs that can be audited at any time.
b) There is a clear audit trail of the use of the BWV with operations and recording details all audit-logged and indexed.
c) Video downloading is protected by an advanced encryption standard (AES) with encrypted keys specific to the relevant device base station.
d) The camera wearer cannot access, view or delete any recordings directly from the device, there is no view, copy or deletion ability available to users.

Data will only be captured during an act of aggression when the staff switch the BWV devices on, as the device is not constantly storing data. The BWV device will be constantly operating but will only store data if the record button is pushed by the staff member. If record is pushed, the BWV device will buffer up to 30 seconds prior to the record button was used. Staff will activate their cameras at the start of an incident and under normal circumstances will continue to record until it is no longer 'proportionate or necessary'.

Any footage on the BWV will be stored on each individual device until the data is transferred off the device to a secure back-office system/server within Boston CCTV Suite. This occurs within 2 hours automatically of being placed in the docking station.

Docking stations and dedicated software will be evident in each Council across the Partnership area.

Location of docking stations will be in secure and accessible locations. Once the BWV has been docked, the data transfer process will be automated, encrypted and transferred to the server. This will only transfer data if the record button has been pressed on the BWV device and data is held. Devices will also have a backup to allow for data transfer via a USB cable or secure wireless connection. All recordings will be erased from the individual device once the data has been transferred. The captured images and audio cannot be replayed on the BWV device by the individual staff member.

The device is a sealed unit with no user access to any storage media by the users which prevents ready access to video files in the event of the device been lost, stolen or attempted to be hacked,

The footage/evidence is stored and segregated securely, accessible only by the relevant stakeholders to ensure privacy and evidence security.

The new system will have role-based access levels, aligned to The Councils' information asset owner structure. The specific access levels allow regulated access and permissions to perform various functions.

The Councils have a process in place to redact sensitive information or third-party information, for example through collateral intrusion spillage of coverage by the cameras. This information, which is often generally termed as PII (personally identifiable information), includes images of faces of individuals and vehicle registration number plates. See below for redaction during subject access requests.

The devices have been chosen partly due to the high quality of images that it records. These are full 1080p HD images recorded through a wide-angle lens and a dual microphone captures audio recordings.

The devices will be securely attached via original branded accessories which are designed to avoid accidental loss and malicious removal, have secure and quick release mounts attached to uniform clothing.

The attachments permit only limited movement of the device when the user is in motion and are designed to ensure that the device is always pointed correctly at the operators focus of attention.

Only officially procured Body Worn Video devices can be utilised by staff. Under no circumstances must any privately-owned BWV devices be used to capture evidence by any Councils employee.

BWV footage that staff record is stored for 30 days. If the data is required for prosecution purposes, the data is stored in an electronic folder for use by the Police and is then destroyed when a prosecution is complete. The data is encrypted when it is electronically transmitted to the cloud, remains encrypted whilst in store and encrypted when it comes back to us if it needed by the Police. If footage is identified and utilised for specific purposes (for example law enforcement), footage will be retained for 7 years from closure of investigation.

The UK GDPR does not prevent The Councils sharing personal data with law enforcement authorities (known under data protection law as "competent authorities") who are discharging their statutory law enforcement functions. The UK GDPR and the DPA 2018 allow for this type of data sharing where it is necessary and proportionate.

Therefore protocols for distributing or sharing BWV will be in place and will cover sharing data for a legitimate purpose i.e. Police, IPCC, Health and Safety Executive etc. and will include processes for releasing data for subject access requests which will include visual data redaction, audio data redaction and output data.

A stand-alone data sharing agreement will be/has been created to cater for the sharing of these images with partner agencies such as the Police.

Primary requests to view data generated by a BWV device are likely to be made by third parties for any one or more of the following purposes:

i. providing evidence in criminal proceedings

ii. the prevention of crime

iii. the investigation and detection of crime (may include identification of offenders)

iv. identification of witnesses

v. Internal Gross Misconduct enquiries.

(Information is only released to third parties on receipt of the appropriate REQUEST FOR DISCLOSURE OF PERSONAL INFORMATION - Schedule 2, Part 1 (2) Data Protection Act 2018 form completed by the appropriate police/organisation rank.

The same applies to other law enforcement agencies.

Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

a. police

b. statutory authorities with powers to prosecute, for example Customs and Excise, Trading Standards

c. solicitors

d. claimants in civil proceedings

e. accused persons or defendants in criminal proceedings

f. other agencies, (as agreed by the Data Controller and notified to the Information Commissioner) according to purpose and legal status.

Upon receipt from a third party of a bona fide request for the release of data, the Councils BWV Information Governance lead shall:

i. Not unduly obstruct a third party investigation to verify the existence of relevant data,
ii. Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order. A time limit shall be imposed on such retention, which will be notified at the time of the request.

Where requests fall outside the terms of disclosure and Subject Access legislation, the IG lead, or nominated representative, shall treat all such enquiries with strict confidentiality.

BWV footage may also be shared internally, for circumstances where there is a desire to review allegations made under a complaint, disciplinary process or serious incident investigation. This BWV footage will only be shared if appropriate to do so, will only be viewed by those individuals when it is necessary for them to view the footage and will be reviewed on a case-by-case basis.

The BWV procurement process includes suppliers protocols on accessing risk factors associated to storage media options e.g. removable media or non-removable media, accidental loss of media, interference on data physical damage to media, compromise to continuity, flexibility of data transfer options. Encryptions will be fully accessed to review direct access to data, data or metadata that is scrambled exclusive to a supplier, same access code or key to encrypt and decrypt data etc. Risks will include data accessible by an unauthorised party, sharing data with external agencies etc.

The device would be encrypted and there is a limited amount of captured information stored on the device's internal memory and requires specific docking facilities to access the footage. In addition it is important to note that the recording itself is encrypted, as it records,

The devices comply with the AES256 Advanced Encryption Standard. Only the software can decrypt it, so when it is uploaded to Council storage systems, the recording remains encrypted.

Footage will only be accessed by authorised and nominated Council staff via PCs with personal logins, and only held past 30 days if it is deemed as evidential.

Existing arrangements are in place for CCTV data access and disclosure and will remain unchanged, i.e. footage will be supplied for evidential purposes only. It will be decrypted using the software and emailed to IT requesting it to be put on a password protected DVD/CD. Footage must be requested by authorised police staff or other statutory agencies with legitimate powers to access the information. Immediate supply for life/death, detection of crime incidents will be provided in written request of a police officer of at least Inspector rank.

In all cases a REQUEST FOR DISCLOSURE OF PERSONAL INFORMATION - Schedule 2, Part 1 (2) Data Protection Act 2018 will be required from the Police to release BWV footage. The Master copy will be retained securely on-site with the Information Governance Team.

The footage captured can be easily located once uploaded to a server.

No facial recognition is integrated into the system and it does not have the ability to be watched live.

The "User Manual" and 'Standard Operating Procedures', given to all staff who use BWV devices, demonstrates in simple terms, how the system should be used, how information is captured on a BWV device, processed, and then deleted if not required.

8. Does the system's technology enable recording?

Yes

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

See above, the recording, images and audio, will take place on the individually worn BWVs. It will then be uploaded onto designated PCs within the Councils CCTV suite where it will be retained during assessment by authorised staff members.

9. If data is being disclosed, how will this be done?

This will be a combination of on-site visiting by requestors or where the identity is known via copies of footage sent through encrypted email systems.

10. How is the information used?

The camera acts as an independent witness. The camera records the footage onto an internal storage device. At the end of the Council officer's shift the footage is uploaded to a secure

location so it can be used as evidence at court or other legal proceedings or deleted if it's not needed. It is not monitored in real time nor used to compare with reference data of persons of interest through processing of biometric data, such as facial recognition. It is possible that recorded data may be disclosed to authorised agencies to provide intelligence to support the prosecution or detection of offenders.

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted

Consultation method

Views raised

Measures taken

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

What is your UK GDPR lawful basis for processing (see Appendix 2 below and consult your IG department)?

Lawful basis

We process data in accordance with Article 6(1)(e) of the General Data Protection Regulations, this is because the processing is necessary for the performance of a task carried out by The Councils in the public interest or in the exercise of official authority vested in The Councils. This is grounded in UK legislation and investigations in respect of a number of types of offences, for example benefit fraud, fly-tipping, fraudulent use of a blue badge, health and safety offences, noise nuisances, irregular school attendance, issues with taxi licensing and breaches of planning notices assessment meet our objectives, is in the public interest, and is proportionate and legitimate to the aims pursued.

As such The Councils may rely on this lawful basis because it is necessary for them to process personal data either in the exercise of our official authority (covering public functions and powers as set out in law) or to perform a specific task in the public interest (as set out in law). These include:

- The main legislative requirement of The Councils is founded in The Local Government Act 1972 (LGA 1972), which gives local authorities power to prosecute criminal offences investigated by their own departments.

Other legislation includes:

- Health and Safety at Work Act 1974 – The Councils are required to assess risks to staff and ensure that adequate control measures are in place. A regular review of the corporate risk assessment with regards to violence and aggression to our staff is regularly carried out by the H & S teams, and the associated action plan is regularly updated. The front-line officers working environment is diverse and challenging in that there is very limited scope for the implementation of basic control measures such as improving the security to prevent attacks, workplace space, lighting etc., therefore alternative controls such as BWV must be considered.
- Offences against the Person Act 1861
- The Criminal Justice Act 1988
- The Crime and Disorder Act 1998
- The Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- European Convention of Human Rights, European Convention on the Rights of the Child and Human Rights Act 1998 – In general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's (including a child's) privacy. The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, whilst others are qualified, meaning that it is permissible for the state to interfere with the right provided that the interference is in pursuit of a legitimate aim and the interference is proportionate. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR
- The use of BWV is 'an interference' and must always be justifiable, therefore the actions of the Councils must be justifiable, have a legitimate aim and the use of video / audio must be proportionate to achieving this.
- The Councils will carry out a full Data Protection Privacy Impact Assessment in order to address any issues raised by this Article and introduces safeguards associated with how the Councils deploys this equipment in both private and public arenas.
- Freedom of Information Act 2000 – grants a general right of access to all types of recorded information held by public authorities, which will include digital images such as those recorded by body worn video. However in most cases this will be personally identifiable information and exemptions would be used e.g. Section 40 – Personal Information and then the request would be placed under a SAR. Procedures are in place to manage subject access requests in respect of video and audio captured using BWV equipment. Each request will be accessed case by case.

Other guidance includes:

- Home Office – Safeguarding Body Worn Video Data (Published October 2018): Supporting Guidance Document
- Information Commissioners CCTV Code of Practice
- Information Commissioner Guidance – Body Worn Video

Processing special categories of personal data:

The lawful basis to process special category data with BWV is found in Article 9 UK GDPR Article 9 where the processing is necessary for reasons of

(b) Employment, social security and social protection (if authorised by law)

(c) Vital interests

(f) Legal claims or judicial acts

(g) Reasons of substantial public interest (with a basis in law)

(h) Health or social care (with a basis in law)

Operational staff will only deploy BWV recording under the defined operational requirements (where there is a risk of violence, aggression or assault or criminal acts against staff) and we need to ensure that the use is proportionate, legitimate, necessary and justifiable. In every case where the BWV is activated, the staff member involved must be prepared to justify its use.

Article 10 of UK GDPR allows the processing of personal data relating to criminal convictions and offences.

Paragraph 10 of Schedule 1 of the DPA 2018 provides a condition for sharing special category data or criminal offence data where it is necessary for the prevention or detection of unlawful acts, and where asking for consent would prejudice that purpose.

Paragraph 2 of Schedule 2 of the DPA 2018 provides an exemption (the "crime and taxation" exemption) from the UK GDPR's transparency obligations and most individual rights, but only if complying with them would prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders. This is not a blanket exemption, and The Councils must consider it on a case-by-case basis.

The Councils fully understands that the utilisation of BWV cameras must be lawful and fair. This means we must have an appropriate legal basis or justification, for using BWV as required by Article 6, 9 and 10 of the UK GDPR and as outlined above.

Any footage recorded can only be processed for purposes that are otherwise lawful and fair towards affected data subjects. Any BWV devices implemented will not be unduly detrimental, unexpected, misleading, or deceptive to individuals who are recorded and protocols will be put in place to support this.

The Councils believe that BWV devices are necessary for achieving the purpose of reducing unprovoked attacks on Council personnel by members of the public but also understands that we have to have clear policies, procedures and training programmes to support their lawful use.

We will ensure that we act with integrity and transparency with their use. This offers protection for both the public and our frontline staff. We will ensure the existence of appropriate safeguards, which may include encryption or pseudonymisation.

It is further recognised that consent will not be an appropriate legal basis for the use of BWV devices as gathering the consent of each person recorded would not be possible or practical. In the event that someone requests that the BWV be switched off, the staff member may 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.
- Recorded material can be accessed on request in writing in accordance with the DPA, 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.

However, a colleague failing to record an incident may be required to justify the actions as vigorously as any colleague who chooses to record a similar incident.

In all cases, recording can only be justified when it is relevant to the incident and necessary in order to gather evidence.

Other compliance protocols and supporting legislative frameworks:

The Data Protection Act 2018 defines personal data as any information relating to an identified or identifiable living individual and UK GDPR allows for the disclosure of personal data to, for example, to Police when the purpose is to prevent and detect crime.

Policy, Procedures & Training:

13. Training In The Use of BWV Devices / Docking Stations:

All operational staff who have been identified as potential users for BWV devices, and their managers, will be trained in how to use the devices.

The training includes:

a) Clearly set out the circumstances in which The Councils staff may or may not use the BWV devices.

b) Applicable legislation and legal requirements of using BWV devices in a public area, privacy, data protection, information governance etc.

c) Explain the purposes for which any video and audio footage is obtained and how it will be processed appropriately.

d) The importance of compliance with human rights, equality and disability requirements, best practice and legislation including the need to exercise care when deploying surveillance systems, particularly in relation to collateral intrusion, recording in areas which generally attract privacy (such as bathrooms) and recording vulnerable individuals and/or children.

e) Framework and reasons for implementation of devices throughout the Councils, including who in The Councils is entitled to view and process the surveillance footage, and the circumstances for which access should be granted.

f) How to mount the device on the body

g) How to operate the device, turning on/off and various functions

h) When to operate the recording function and the parameters of permitted use

i) Permissions of use, how to alert the public recording is about to commence and reasons why

j) Maintenance and charging of the device

k) How to use the device for information and data upload/transfer

l) The timeframe for uploading of information and data

m) How the information and data is stored and erased from the devices

n) Implications for misuse for example equipment and

o) That recordings must be retained and handled in accordance with The Councils BWV policy and that any breach of the BWV policy may render the user liable to disciplinary action and/or adverse comment in criminal proceedings.

All personnel must attend a full training session prior to operating the BWV device in an operational environment.

All personnel must sign to acknowledge they have been trained in the use of BWV devices and understand their legal responsibilities in its use.

Records of this training will be held centrally for audit and accountability purposes. All personnel must attend a full training session prior to operating the BWV device in an operational environment.

The implementation of BWV will require the support of policy and procedural documents along with a training programme to ensure the equipment is used appropriately and within the statutory requirements and guidance.

All personnel must sign to acknowledge they have been trained in the use of BWV devices and understand their legal responsibilities in its use.

Records of this training will be held centrally for audit and accountability purposes.

14. Post-event storage:

- All images captured by BWVC will be handled securely in accordance with The Council's CCTV retention procedures where products with no evidential or other lawful value will be retained for a maximum of 30 days with authorised officers being responsible for destruction of data.
- Any product of evidential or other lawful value will then be stored, retained, reproduced and disposed of in accordance with prevailing legislative requirements and The Council's Data Retention Policy.
- All footage recorded to the BWV unit will be downloaded as soon as practical. Evidential footage downloaded will be saved on the relevant stand-alone BWV computer as per the approved procedure.
- It will be identified by exhibit/unique reference number.
- As soon as reasonably practical, a CCTV Operator will make two DVD copies. The first will be a 'master copy' which will be sealed, labelled. The second will be a 'working copy' for investigation and file preparation purposes. DVDs should be retained in line with authority's evidential retention policy.

The system has been properly set up to retain data for the correct retention period (maximum 30 days, before automatic deletion).

Transparency

15. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

The BWV is worn in a prominent position and not hidden in any way. Prior to commencing recording, wherever possible, the Councils Officer will inform the individual that they are about to switch on their device. This will ensure that there are no surprises for individuals if footage is subsequently used.

The Councils Privacy Notice reflects the potential for BWV usage.

The Councils may include reference to the potential/use of BWVC devices within letters, Notices, Orders or other communications to individuals, groups or businesses

16. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

When capturing information on these devices, staff will only do so in order to fulfil the legitimate purpose, which is to reduce violence and aggression towards staff. Data will only be

accessed and stored when a member of staff completes an incident report form and advises that footage is available. Footage will then be accessed by one of the authorised and nominated Council staff, and stored as it is deemed as evidential. Footage may then be shared with other organisations as detailed above.

Use of BWV is subject to policy and procedural compliance, along with a training programme to ensure the equipment is used appropriately and within the statutory requirements and guidance, in particular:

- Body Worn Video (BWV) Policy.
- Body Worn Video (BWV) Procedures.
- Body Worn Video (BWV) Standard Operating Procedure.
- Training programme for all designated users and applicable line management.
- Protocols will also be developed to ensure that no appropriate use of the BWV is being used. For example, audits of files from BWV devices will be undertaken on a regular basis to ensure no inappropriate use.

16. How long is data stored? (please state and explain the retention period)

All images captured by BWVC will be handled securely in accordance with The Council's CCTV retention procedures where products with no evidential or other lawful value will be retained for a maximum of 30 days with authorised officers being responsible for destruction of data.

Any product of evidential or other lawful value will then be stored, retained, reproduced and disposed of in accordance with prevailing legislative requirements and The Council's Data Retention Policy.

All footage recorded to the BWVC unit will be downloaded as soon as practical. Evidential footage downloaded will be saved on the relevant stand-alone BWV computer as per the approved procedure.

It will be identified by exhibit/unique reference number.

As soon as reasonably practical, a CCTV Operator will make two DVD copies. The first will be a 'master copy' which will be sealed, labelled. The second will be a 'working copy' for investigation and file preparation purposes. DVDs should be retained in line with authority's evidential retention policy.

The system has been properly set up to retain data for the correct retention period (maximum 30 days, before automatic deletion).

Retention Procedure

See above, Data is automatically deleted after 30 days unless required for the prevention or detection of crimes, under these circumstances authorised persons may override the retention period, e.g. retained for prosecution (see above).

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Cameras are fully encrypted and can only be linked to designated PCs within the CCTV Suite.

Data collected from BWV cameras is not accessible to any other parties other than other authorised The Councils officers. The data is only uploaded to The Councils secure server.

Only nominated The Councils officers will be able to access the footage to view recordings.

The system used will be regularly tested to ensure its efficiency in protecting the footage captured. Procedures will be regularly checked to ensure best practices are followed, to identify problems in the procedures and to amend / update them as necessary.

The Councils staff must also undergo mandatory Cyber Security training.

Misuse of the data constitutes serious misconduct and will be robustly dealt with should it ever happen. Auditing systems are in place to deter any such wrong doing and to identify it, should it happen.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

The Councils has a relevant suite of policies and procedures for Subject Access Requests and Data Requests which are followed if a request is received.

The SAR may include the release of the BWV footage as well as other supplementary information. While a Data Subject is entitled to their personal data they are not entitled to another person's personal data especially if this could cause that person harm. if the information or images captured contains third party images that are unrelated to the initial request, these images should be obscured under the Data Protection Act (DPA) and UK GDPR.

The Council has implemented suitable redaction techniques to mitigate inappropriate and excessive disclosures and in line with routine SAR responses, will consider whether it is suitable to disclose third party data to the requestor (which may include seeking third party consent). Where necessary this may include redaction techniques to remove non-personal information, for example blurring, cropping, masking or using a solid fill to completely obscure parts of the footage.

Where necessary metadata will be removed from such disclosures.

Redaction and pixilation of BWV will used where required, so that data released under a SAR relates only to that person.

Any internal/external release of BWV footage to support secondary processing for such investigation as employee related investigations, personal claims etc. will be managed in line with routine data protection protocols.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

Body-worn recording devices worn by officers are the most appropriate way of collecting audio and video data during potentially violent or abusive encounters with members of the public BWV has the ability to capture footage and audio in close proximity to individuals, and whilst the potential to be more intrusive than conventional CCTV systems.

However, there is little alternative less intrusive methods when considering the spontaneous, instant reactions of members of the public who may be investigated by our staff.

The cameras are very easily identified, attached onto the front of clothing or a uniform.

Due to BWV's increasing affordability, many different organisations in the public and private sectors now purchase and use such equipment.

BWV devices have the ability to be switched on or off, but it is important to know when and when not to record.

Our staff will not routinely activate the cameras as this is likely to be excessive; and may inadvertently capture others going about their daily business, as well as the individual who is the focus of their attention.

Therefore we advocate that it is appropriate for staff to switch on their BWV camera when they believe an individual is being aggressive towards them, but not when an individual is merely responding not questions or enquiries in a peaceful manner.

The BWV we have procured provide a dedicated, officially procured, recognised and supported type of recording device that meets the needs of our own staff and ensures best possible compliance with data protection and security.

The use of body worn video devices is well established amongst public sector organisations delivering services where staff members may be exposed to increased risks of assault and abuse. The importance of providing protection for staff members supports the use of this system.

Part 2: Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system.

Describe below any specific data protection risks and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of harm** 1. Rare 2. Unlikely 3. Possible 4. Likely 5. Almost Certain	**Severity of harm** 1. Insignificant 2. Minor 3. Moderate 4. Major 5. Catastrophic	**Overall risk** 1. Low 2. Medium 3. High 4. Extreme	**List the various controls that have been or will be put in place to mitigate the risk prior to commencement**	**Effect on risk** Reduced Accepted	**Residual risk** Low Medium High
If the purpose of Body Worn Video is not clear to the public, there is a risk that it may be seen as an unjustified intrusion on privacy. The public may feel that they have not consented to the use of the technology. There may be public distrust. Vulnerable groups may be disproportionately impacted.	**3**	**3**	**Med**	Information Governance and Equality expertise sought on an ongoing basis. Privacy notice will be updated for Public, Children and separate one for CCTV. BWV assets added to The Councils information asset register. Legal basis for processing is clear has been identified under Article 6, Article 9 and pursuant to Article 10 of the UK GDPR • Footage provided to the police, IOPC, Health and Safety Executive or other statutory agencies for criminal investigation; The Councils copy securely destroyed after 2 years or following the cessation of any proceedings.	**Reduced**	**Low**

				• Footage required for internal/external employee related investigations, personal injury claims (and identified as secondary processing); securely destroyed after one year. • Unmarked footage; securely destroyed after 30 days. • Recorded material is The Councils information and can be accessed on request in writing in accordance with the data protection legislation unless an exemption applies in the circumstances (Subject Access). The individual BWV operator will consider on a case-by-case basis whether or not to switch the BWV on or off. There should always be a presumption to record if the operation guidance has been met unless the circumstances dictate otherwise. A member of staff failing to record an incident may be required to justify the actions as vigorously as any member of staff who chooses to record a like incident. In all cases, recording can only be justified when it is relevant to		

				the incident and necessary in order to gather evidence.		
If the purpose of Body Worn Video is not clear to staff there is a risk that it may be seen as an unjustified intrusion on privacy, wellbeing may be impacted, there may be distrust, lack of support or reassurance for The Councils. Councils and relationships with management and staff associations may be impacted.	**3**	**3**	**Med**	Purpose will be made clear during staff training programmes and as part of the associated policies and procedures. Trade Union colleagues have been engaged with the project from the beginning.	**Reduced**	**Low**
Compliance related risks, i.e. failure to adhere to data protection legislation, potential fines from the Information Commissioner for incorrect processing or breaches, privacy requirements, human rights legislation and / or sector specific legislation or standards. This may leave The Councils open to the risk of fines, reputational risk, project failure etc.	**3**	**4**	**High**	BWV is a relatively new technology being deployed by The Councils. However we recognise the concerns regarding privacy issues. Accordingly, this technology will only be deployed in an overt manner, using trained staff and in defined operational circumstances. All captured data will be processed to ensure total compliance with the Data Protection and Human Rights legislation, and retained and subsequently disposed of in	**Accepted**	**Med**

				accordance with the relevant policies and procedures. • A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced. • A published point of contact for information, complaints and concerns. • Where appropriate there will be the required CCTV warnings and signage on all devices and vehicles. • Training for staff in order that they can confidently engage with members of the public on the matter.		
There is a risk that staff will use the device in circumstances which are not appropriate, continuously, or not within the defined operational requirements.	**3**	**4**	**High**	The Councils will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. At all stages it will comply with the Data Protection Act and other legislation such as Human Rights legislation, there will be adherence to the requirements of Article 6 (Right to a fair trial) & in respect of Article 8	**Accepted**	**Med**

				(Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured & processed to achieve a legitimate aim as detailed.		
There is a risk that over a period of time project creep will occur, or requests could be made to use the data for other purposes.	**3**	**3**	**Med**	The Councils will only deploy this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary and justifiable. Staffing measures to prevent mission creep or misuse of the process include: • Rigorous Staff checks/vetting procedures (Police checks and DBS). • Robust contracts with confidentiality clauses. • Operatives are given specific induction, training and refresher training in use of the equipment. Recording will be initiated when the Council staff become involved in interactions with the general public who are assessed as been threatening or abusive. Recording is carried out overtly. No covert surveillance is to be carried out using personal issue BWV.	**Reduced**	**Low**

				Recordings will be automatically deleted as detailed in the Councils' Data Retention schedule.		
There is a risk that inappropriate or excessive data will be held, for example: • Audio – this technology allows the capture of both video and audio data which differs from CCTV. As a result persons may feel that they have not consented to the use of the technology. In some instances, the camera itself may not be pointing in the direction of the main incident but that the surrounding audio will still be captured. • Collateral intrusion – in this context extends to the capturing of the movements and actions of other persons when this equipment is being used. It is inevitable that in some circumstances this will occur.	**3**	**3**	**Med**	Audio recording - as previously stated BWV is a new technology and is seen to have major benefits of capturing evidence in an indisputable format. In order to ensure that all aspects of an incident are captured, this requires the essential inclusion of audio information in order for this to be complementary to the video data. The other important aspect of the addition of audio information is that in some instances, the camera itself may not be pointing in the direction of the main incident but that the audio will still be captured. This has a significant advantage of protecting all parties to ensure that the actions of the Council staff were totally in accordance with the law. Equally, in some instances, the presence of only video evidence without the added context that audio, can fail to adequately provide the full context, for all parties, of an incident or interaction.	**Reduced**	**Low**

• Increase in the quantity of data – BWV is a relatively new technology and is seen to have major benefits of capturing evidence in an indisputable fashion. Accordingly, there will be more data potentially being captured. • Inability to switch off recording – there is a risk that a member of staff may not be able to switch off the recording due to an incident or operational needs.				Collateral intrusion - 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 aggressor. In circumstances where individuals are captured in any video or audio information and they are unrelated to any offence under investigation, their identities will be protected and anonymised especially should the matter be presented to a court. Increase in the quantity of data – BWV is a relatively new technology and is seen to have major benefits of capturing evidence in an indisputable format. Accordingly, there will be more data potentially being captured but the appropriate safeguards, by adherence to legislation and guidance, will ensure that only information that passes a strict test, of being required for a legitimate purpose, can be retained. Inability to switch off recording – staff will be advised to make every effort to		

				ensure devices are switched of when not required. • A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced. • Training for staff in order that they can confidently engage with members of the public on the matter.		
• There is a risk that a member of staff will fail to dock the device. • There is a risk that the device will not automatically download. • There is a risk that the data will not be marked evidential and be automatically deleted. • In the event that a system is purchased that incorporates the ability to wipe the device remotely, there is a risk that evidential data could be accidently erased.	**3**	**3**	**Med**	Equipment will be installed and maintained as per manufacturer's instructions. Any device issues / failures / incidents will reported and investigated. • A Body Worn Video Policy, Procedure and Standard Operating Procedure will be introduced. • Training for staff in order that they can confidently engage with members of the public on the matter. Following an activation the member of staff will be returned to the premises,	**Reduced**	**Low**

				follow a 'check-in' process and 'dock' it into a dedicated port that automatically downloads all the captured information onto the server. This information cannot be deleted or altered and is encrypted. The member of staff will then complete an incident report form which will flag up that data needed to be retained. One of the Councils trained and authorised officers will then identify the elements of captured data to be retained via the software and 'mark' the section appropriately. It will then be backed up on to the primary back-up and then secondary back-up if required. Once completed, the contents on the device are deleted and retained as stated. All other material will be automatically erased after 30 days. Training for authorised officers will include information on the remote wipe function and risks if appropriate.		

There is risk that data will be held for inappropriate length of time.	**3**	**3**	**Med**	Any information captured on a device, which is deemed to be non-evidential will be automatically deleted after 30 days. The only rationale for any retention beyond an immediate disposal include circumstances where staff have been subject to violence and aggression in the course of their duties, and there is a desire to review the incident as part of a police investigation. In these circumstances, The Councils' Information Governance Team will retain a master copy and it will be stored in line with the Councils' Retention Scheme. Data within the evidential category which has been passed to the police, courts etc. will be reviewed and disposed of, in accordance with timeframes within the justice system or 2 years following the cessation of proceedings.	**Reduced**	**Low**
• Recording in private dwellings – If the purpose of Body Worn Video is	**3**	**3**	**Med**	Recording in private dwellings – It is widely recognised that citizens are	**Reduced**	**Low**

not clear to the public, there is a risk that it may be seen as an unjustified intrusion on privacy. • State of undress – there is a risk that footage may show persons in a state of undress. • Access requests – there is a risk that there will be an increase in requests for data and The Councils will not be able to process the requests in a timely way.				likely to have a strong expectation of privacy especially in their own homes. Indeed this is contained with Article 8 of the ECHR (a right to respect for a private and family life) and under normal circumstances BWV would not be used in private dwellings. However if the user is present at an incident in a private dwelling, and there is a risk of violence and aggression, then there is a genuine purpose and this equipment is able to be used. The user will be mindful to exercise discretion and recording should only be used when it is relevant to the incident and necessary in order to gather evidence, all recordings require a lawful basis in order to justify infringement of Article 8. In circumstances where an occupant of the premises objects to the recording taking place but where an incident is taking place staff are recommended to continue with a recording but explain their reasons for doing so. These reasons might include:		

				• That an incident has occurred requiring police to attend. • That the member of staff continued presence might be required to complete the enquiries. • There is a requirement to secure best evidence of any offences that have occurred and that the video/audio evidence will be more accurate and of a higher quality and therefore in the interests of all parties. • That continuing to record would safeguard both parties, with a true and accurate recording of any significant statement made by either party and of the scene • That the incident may reoccur in the immediate future • That continuing to record will safeguard the BWV user against any potential allegations from either party. The Councils is very mindful of the concerns that this raises and will train its users to respect and adhere to these safeguards.		

				When capturing information on these devices, Council staff will only do so in order to fulfil the legitimate purpose, which is to reduce violence and aggression towards staff. Data will only be accessed and stored when a member of staff completes an incident report form and advised that footage is available. Footage will then be accessed by one of the authorised and nominated Councils staff, and stored as it is deemed as evidential. Footage could then be shared with the police, Crown Prosecution Service, Defence professionals and the Courts to support a prosecution. 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 the police. In instances of any dispute, the Court can require the production of the Master copy. This should only be done in		

				liaison with a senior member of the Council. Other various access requests will be dealt with via existing information governance arrangements, i.e. via the Information Governance Team. The Councils will review resources required longer term for the management of BWV data and security related matters.		
• It is also possible that in some circumstances, such as a violent encounter, a device might become detached from a member of staff and fall into the hands of unauthorised persons. This presents the possibility of the data being accessed by an unauthorised individual. • There is a risk that a device will be lost or stolen.	**3**	**4**	**High**	This technology will only be deployed in an overt manner, using trained staff and in defined operational circumstances. All captured data will be processed to ensure total compliance with the Data Protection and Human Rights legislation and retained and subsequently disposed of in accordance with The Councils Policy. Due to the very nature of confrontation and investigations, it is possible that in some circumstances, a device might become detached from a member of staff and fall into the hands	**Accepted**	**Med**

• There is a risk of unauthorised access to and / or unauthorised copying of data. • There is a risk of claims for compensation as a result of data loss. • There is a risk of a cyber-security incident / data being accessed by unauthorised persons. • There is a risk of data loss due to human error, failure to back up server, viruses, network failure, fire, flood etc.				of unauthorised individuals and therefore potentially stolen, with the possibility of the data being accessed by an unauthorised individual. The means of attaching equipment to the member of staff has been subject of much consideration and is designed to physically reduce instances of the equipment being ripped from a member of staff. Attachments to have been fully tested as part of implementation. The impact in terms of any time lost between any actual loss and notification to the Councils, is kept to a minimum. Where a device is lost, it will be reported immediately to the Information Governance Team and or the most senior officer on call. The device is encrypted and there is a limited amount of captured information stored on the device's internal memory and requires specific docking facilities to access the footage. In the event of a loss the Councils intends to have the ability to locate via GPS and remote wipe.		

				In terms of cyber security, a device is docked in order to transfer data, therefore the entire The Councils network would have to be hacked for it to be at risk. Also the device is encrypted and there is a limited amount of captured information stored on the device's internal memory and requires specific docking facilities to access the footage. In addition it is important to note that the recording itself is encrypted, as it records, not the device, to AES256 standard. Only the software can decrypt it, so when it is uploaded to The Councils storage systems, the recording remains encrypted. The software decrypts the recording and stores separately, therefore two versions exist, an encrypted and a decrypted record. The software may also be able to auto purge all decrypted recordings. The procedures and principles applicable to BWV are similar to how The Councils handles requests or court orders for CCTV data. Issues relating to these requests will be referred to the Information Governance Team and		

				escalated through senior management as necessary. Depending on supplier, devices are likely to be docked and data automatically downloaded to central server and is not accessible by staff or line management locally. Footage will only be accessed by one of the authorised and nominated The Councils staff via PCs with personal logins, and only held past 30 days if it is deemed as evidential. The Councils has an ICT resource and expertise as part of project team. Existing arrangements are in place for CCTV data access and disclosure and will remain unchanged, i.e. footage will be supplied for evidential purposes only. It will be decrypted using the software and emailed to IT requesting it to be put on a password protected DVD/CD. Footage must be requested by authorised police staff on the appropriate forms, and collected by hand under signature. Immediate supply for life/death, detection of		

				crime incidents will be provided in written request of a police officer of at least Inspector rank. In all cases a completed REQUEST FOR DISCLOSURE OF PERSONAL INFORMATION - Schedule 2, Part 1 (2) Data Protection Act 2018 form completed by the appropriate police/organisation rank will be required. The Master copy will be retained securely on-site with the Information Governance Team. The Councils Business Continuity Policies, Procedures and Plans are in place. Existing arrangements are in place for CCTV data access and disclosure and will remain unchanged.		

Step 6. SIGN OFF and record outcomes

a. Project Lead / Service Lead

The Project / Service Lead sign-off confirming they have or will:

- *review any consultation responses, provide any required explanation on outcome and explain reasons if decision departs from the views of any stakeholders.*

- *accept and approve any measures outlined in the DPIA and integrate actions back into the project plan*

- *ensure appropriate data sharing arrangements are put in place where data is shared with third party organisations (e.g.: Contracts, Data Access Agreements, Data Sharing Agreements)*

- *consider the need for additional information in The Councils Privacy Notice to inform service users of how their personal data is to be processed; and if appropriate put this in place*

- *keep the DPIA under review*

Project /Service Lead Comments:

- Ongoing monitoring of consultation.
- Mitigations accepted and will be implemented.
- Any necessary additional data sharing agreements will be put in place.
- Privacy notice will be updated.
- DPIA will be kept under review.

Name:	
Job Title:	
Signed:	**Date:**

b. Data Protection Officer (DPO)

The DPO should:

- *Advise on compliance, 'step 5' mitigating measures and whether processing can proceed.*

- *Ensure the DPIA is added to central DPIA Register (by Information Governance)*

Summary of DPO advice:

The detailed background, risk descriptions and mitigating measures (to reduce or eliminate risks) in this DPIA indicate that there are appropriate technical and organisational measures in place for The Councils to lawfully utilise BWV devices as described. The DPIA is sufficient to implement the data protection principles effectively and safeguard individual rights in this case.

Name:	
Signed:	**Date**:

c. Information Asset Owner (IAO)

The IAO should:

- *Consider and approve any residual risks. If accepting any residual high risk, you should consult the Information Commissioner's Office (ICO) before going ahead.*

- *Ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training*

- *Make arrangements for any new systems to be added to the Information Asset Register (IAR) or update an existing entry to reflect new processing*

IAO Comments:

Name:	
Title:	
Signed:	**Date**: