Privacy Impact Assessment of the use of Body Worn Video

Parking Services

A Privacy Impact Assessment (PIA) is a tool which can help the Council identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy.

This PIA reviews the implementation of the use of Body Worn Video by Civil Enforcement Officers within the Council's Parking Services Department.

Privacy Impact Assessment – Screening questions

These questions assist the Service in identifying if a Privacy Impact Assessment is necessary.

If the answer to one or more of the questions below is 'yes' please complete the Privacy Impact Assessment (Appendix 3 and return to the Information Management Team (IM) (informationmanagement@sheffield.gcsx.gov.uk).

1. Will the project involve the collection of new information about individuals (Personal Data)?

Yes – new collection of video though use of body worn video.

2. Will the project compel individuals to provide information about themselves?

Yes – as body worn video is activated during an incident individuals are captured without initial provision of consent.

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information (including Council staff)?

Yes – this is new data collection and any provision to management staff or the police will be new processing.

4. Are you using information about individuals for a purpose it is not currently used for or in a way it is not currently used?

Yes – new processing as body worn video has not been used previously in the Council

5. Does the project involve you using new technology which might be perceived as being particularly privacy intrusive? E.g. Use of biometrics or facial recognition? Any such initiatives should be raised initially with the Information and Knowledge Management time to allow for consideration of any specific corporate risks at concept stage.

Yes – Body worn video activated during an incident without consent of the individual is considered privacy intrusive.

6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Limited – likely impact is use of footage to instigate and as evidence of a report of criminal activity to Police.

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. Health records, criminal records or other information that people would consider particularly private?

Yes – potential capture of criminal activity if footage captures an assault or other criminal act.

8. Will the project require you to contact individuals in ways which they may find particularly intrusive?
9.

No – this is not a form of "contact".

(Source: ICO Privacy Impact Assessment Code of Practice (amended))

Appendix 3 – PIA Template – Full assessment

Privacy Impact Assessment – Full assessment

Project name/ title:	Body Worn Video Project – Parking Services

This document will assist in recording the PIA process and results following completion of the screening questions above. The document should be completed prior to any project commencing and should be updated throughout the course of a projects life.

Name (individual(s) completing the form)	Mark Knight / Ben Brailsford
Position	Information Management Officer / Parking Services Manager
Project sponsor	Ben Brailsford
Position	Parking Services Manager
Team & department	Parking Services – Place
Date of completing form	18th January 2018

Note: The intention is for all completed Privacy Impact Assessments to be published in support of the transparency agenda. Exception will need to be discussed and reviewed by the Information Management Team (IM)

Step 1: Identify the need for a Privacy Impact Assessment

- ***Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. (Purpose – this may be detailed in the executive summary of the associated business case)***
- ***Link to the project proposal if appropriate.***
- ***Summarise why the need for a Privacy Impact Assessment was identified (draw on answers from the screening questions).***

A Privacy Impact Assessment is required for this project due to the likely impact on the privacy of individuals captured by the body worn video. This is personal information (video footage) that has not been captured in this manner before. The majority of information captured by body worn video will be collected without the explicit consent of the subject due to the likely nature of the interaction. The main third party use of this footage is likely to be the provision of footage where incidents are believed to be of such a nature as to require referral to the police. As the cameras are indiscriminate and likely to capture individuals not subject to the concerns of the Civil Enforcement Officer (CEO) which would likely be considered privacy intrusive.

The capture of footage where a CEO has concerns about the current or likely escalating behaviour of an individual is likely to have a significant impact on that individual, particularly if that footage is then shared with the Police for further action after purported criminal

behaviour.
This technology will be utilised to support the evidence gathering and as a diffusion technique for the management of incidents. Parking Services are aware of approximately 214 physical or serious threats annually (Oct 2016). Trend analysis suggests such incidents are rising and that body worn video can act as deterrent to abuse against CEOs[1].

Sheffield City Council has a corporate responsibility to protect the health and safety of its staff. Body worn video is a tool to aid in the diffusion of potential incidents and also provided an opportunity to produce evidence of criminal activity against a CEO.

Step 2: Describe the flow of information

- ***The collection, use and deletion of personal data should be described. You may want to refer to a flow diagram to explain the data flow (See PIA guidance for example)***
- ***An estimation should be made in regard to the number of individuals who are likely to be affected by the project including service users, partners and staff where applicable***

Information (footage) is to be collected on occasions when CEOs perceive a situation is occurring where they feel threatened or likely to face physical or verbal harm.

The activation of cameras should only occur on occasions as noted above and within the associated guidance for relevant staff. Footage is not continuously recorded in order to reduce privacy concerns and only activated when there is appropriate cause.

Once activation has occurred, and on returning to base, the member of staff will pass the device to the returning officer who will download the footage. At this point a decision will be made whether the footage will be:

1. Deleted (physical deletion of memory on the device/ MicroSD card provided with device and associated systems). The devise should automatically wipe on download, but this should be checked upon return or receipt of the device by the CEO.
2. Retained as evidential footage where the Police have been involved and may reactively request the data to investigate the incident concerned. Where applicable footage will be provided proactively to Police as part of the reporting of a crime. Footage will then be deleted unless there is a specific reason for retention which will require review after the standard 14 days retention period.
3. Retained as non-evidential footage pending further investigation or likely complaint from the member of staff or the member of the public captured by the footage

Where footage is retained it will generally be held for a prescribed period of 14 days.

1. At the end of every shift all devices and associated storage must be cleared of footage via upload, if applicable.
2. Where an incident is reported to police and a copy of the footage has been proactively disclosed to police footage should be weeded unless there is a specific reason for retention. Any retention decision should be recorded for audit purposes using the relevant tracker.
3. If a decision is made to retain footage without disclosure to police, footage (i.e. for likely complaint investigation from the officer or member of public identified) should be

[1] See City of London Council report:
http://democracy.cityoflondon.gov.uk/documents/s58442/Body%20Worn%20Cameras.pdf

retained until the conclusion of the related investigation and subsequent appeal process/period and an auditable record of the retention maintained via the relevant tracker.

4. No footage should be retained for excessive periods without consultation with the Council's Information Management Team

Note: Any data retained will only be kept until all internal investigations and associated appeals have been completed. Any exceptions must be discussed with the Council's Information Management Team.

Parking Services estimates that a maximum of **300** activations will be made each year based on current incident referrals to management within the service and associated interactions with the Police. This number may be lower due to the intended impact of BWV acting as a deterrent to incidents of abuse against CEOs.

The full process for the use and management of body worn video footage is detailed in the related *Body Worn Video Policy and Procedure.*

Compliance with relevant legislation

To enable compliance with relevant privacy legislation the following considerations must be made. This element of the PIA process will assist with the identification of risks within the next section of the PIA.

There may be project specific legalisation or codes of practice which should be added to this section of the PIA.

Question	**Response**
Data Protection Act 1998 – Principle 1 Fair and Lawful Processing	
How will individuals be told about the use of their information?	Information will be available on the Parking services area of the Council website noting the use, retention, disposal and access regimes for body worn-video. This will include the provision of a fair processing notice, associated policies and a sequence of FAQs to assist members of the public and relevant contact details for further enquiries; together with the publication of this assessment upon completion. When it is safe to do so officers must provide a verbal privacy notice i.e. provide the name of the Data Controller (SCC), the purpose for recording the footage, that it includes audio and how to contact us about it (i.e. via details on any related PCN issued). This should be completed verbally and should be captured as part of the recording. Where an officer considers that confirmation of the above details are not appropriate and may inflame the

	situation a record to this affect must be taken for future reference, i.e. in the related Incident Report Form logged with Health and Safety. BWV devices will be worn overtly and not hidden. The device overtly records with a visible indicator light and screen display when active. In addition officers carry identification and insignia which clearly identifies them as a member of SCC. Wherever possible staff will notify the member of the public that they will be/ are recording the incident.
Is the use of personal information covered by a current privacy notice?	As noted above a specific fair processing notice will be held within the Parking Services area of the Council website. A small addition to the Council's Data Protection Registration with the ICO on renewal in early 2018 (text due to be added in red): #crime prevention and prosecution offenders including the use of CCTV and body worn video #people captured by CCTV images and body worn video
Will the information include sensitive personal data? If yes, what type and why? (Sensitive personal data is defined as: r*acial/ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation, commission or allegation of crime*)	Sensitive personal data is likely to be captured particularly where the incident escalated to a form of criminal activity against the member of staff i.e. ABH, use of threatening, abusive or insulting words or behaviour under Section 4 of the Public Order Act 1986 or the *offence of mishandling or falsifying parking documents* under the Road Traffic Regulation Act 1984 s115.
Is personal data provided with informed consent, how will this be noted and what will you do if it is withheld or withdrawn?	Consent will not be provided prior to the capture of footage. Schedule 2 of the Data Protection Act will be met as processing is in the legitimate interests of the Council i.e. to protect the health and safety of our staff and capture potential criminal behaviour. The most likely consideration for meeting a Schedule 3 condition is Section 10 and the associated Data Protection (Processing of Sensitive Personal Data) Order 2000 Sch 1 namely it is in the public interest, necessary for the prevention or detection of crime and must be carried

	out without consent. An individual would not provide consent to recording at the start of capture if an illegal act was likely to occur to avoid self-incrimination.
Human Rights Act article 8 – Right to respect for private and family life/ Schedules 1 & 2 Data Protection Act	Information is only captured in specified situations and for a period where the member of staff feels at risk of harm (physical or verbal). Recording will be limited to that purpose and supports the prevention and or detection of crime a legitimate pursuit in a democratic society. During review of footage responsible officers should assure that footage is captured proportionately and not excessively. Any incidents of improper use of the cameras must be investigated and discussed with the individual officers. Any trends or concerns should then feed into future training and guidance provided to staff in the operation of cameras and situation management.
If consent is not being sought provide an explanation why.	
Data Protection Act 1998 – Principle 2 Information obtained only for one or more specified and lawful purpose	
Is there a clear definition of what the information will be used for? (This should link to the Privacy Notice)	Footage capture, use and destruction will be recorded in an auditable manner. For example staff will record activations and their decision making around the activation of the camera on the 'Report of Incident / Injury / Near Miss' report form or pocket book where applicable. An auditable record will also be retained regarding decision making around retention or deletion linked back to a specific time, date and location of the incident. This will include a log of the reasoning for the extended retention of footage outside normal 14 day parameters and in accordance with the Body Worn Video Policy and Procedures.
Does the project involve the use of existing personal data for new purposes?	No
Will this information be shared with third parties?	Most likely sharing will be with the police supporting the purpose of capture in the prevention and detection of crime.
Is there a legal basis for requesting this information?	Information sharing in this manner will be in accordance with Section 29 of the Act, namely for the prevention and detection of crime.
Data Protection Act 1998 – Principle 3 Adequacy and relevancy	
How will the project ensure only minimal data is collected/collated to meets its goals?	Footage will be limited to the incident only with staff required to switch off the

	recording function once the incident has ceased.
Are processes in place to ensure that only required information is being collected once the project is live?	Review on retention will be by managed within Parking Services and noted in the associated audit log. All footage captured will be weeded from devices on a daily basis upon download of footage (and checked by the following user). Wider retention of footage will be completed in accordance with the related policy and procedures.
Data Protection Act 1998 – Principle 4 Accurate and up to date	
Does system of recording information allow information to be updated, changed or deleted when appropriate?	N/A footage captured will be a visual/ audio record of true interactions and should not be amended or edited. The only exception being in the release of information under a subject access request where footage may need to be redacted to remove third party data.
How, and how often, personal data is be checked for accuracy?	As above not applicable.
Data Protection Act 1998 – Principle 5 Kept for no longer than necessary	
Have retention periods been agreed and able to be set within relevant systems?	Retention periods set as detailed above. All footage captured will be weeded from devices on a daily basis upon download of footage. Wider retention of footage will be completed in accordance with the related policy and procedures.
Data Protection Act 1998 – Principle 6 Rights of the data subject	
How will information held be accessible to people to allow access their own information?	Subject access must be built into the process with individuals informed of their right of access to footage if raised including the project's internet presence. Footage should be made available for review and disclosure under a subject access request from the individual(s) captured in the footage. Technical capability to redact footage of unrelated third parties in any onward disclosure will be considered upon review of the footage held.
Will there be public access to the associated system to allow review and updating of personal information held (with appropriate levels of security)?	No – requests will be made via the corporate subject access route only.
Data Protection Act 1998 – Principle 7 Security of personal data	
What security risks have been identified (may be listed in a separate report) i.e. organisational, access, malicious attacks, physical	• Unauthorised access to the footage data store • Security of the BWV device and associated information is stolen from member of staff • Integrity and or loss of storage

	device used within BWV device if memory card style solution used • Theft of footage from Council premises • Inappropriate access by Council staff • Integration between the device, its cloud file store and the Council's ICT infrastructure
What training is to be available to those obtaining or processing personal information?	All staff are required to complete basic Data Protection Act training via e-Learning. Policies and procedures will be created for staff and managers handling this footage to ensure appropriate processing. CEOs and CCTV Control Room staff will receive training in order to manage information in accordance with the relevant policies and standard operating procedures; together with familiarisation with the body worn video device.
Data Protection Act 1998 – Principle 8 Processing outside of the EEA	
Does any element of the handling of data include systems or locations outside of the European Economic Area (EEA) (i.e. cloud storage of information in the USA)? **If yes**, are documented adequate protections in place?	There is no intention to hold, handle or process data outside of the EEA.

Consultation requirements – Internal and external stakeholders
(This can be completed at any stage within the project and should be reviewed if there are any substantial changes to the project that will impact on the privacy of individuals)

- ***Explain what practical steps you will take to ensure that you identify and address privacy risks to and with the consultees.***
- ***Who should be consulted, internally and externally?***
- ***How will you carry out the consultation? – this should link with any other project consultation process***

Links can be made to the project management process and project consultation process.

The major tool for identifying and responding to privacy issues and risks in this project is through the use of this privacy impact assessment. As part of this process there is engagement with the Council's Information Management Team who lead on Information Governance including Data Protection compliance.

Consultation has included Trade Unions and Human Resources in regard to the privacy issues for CEOs in the recording and retention of footage of their interactions with members of the public.

Discussions have been held with the Information Management Team in regard to the Data Protection issues involved together with the production and considerations within this document.

Step 3 Risk Assessment

No.	Privacy risk	Risk to individuals	Compliance Risk	Corporate Risk	Solutions	Result	Approved Solution	Approved By
1	Inappropriate capture of info.	Excessive processing	DPA all principles HRA article 8	Regulatory action, reputational damage and loss of trust in management of personal data	Training of staff and having robust guidance on activation for staff and particular focus on ending the recording when the incident has been resolved or otherwise come to an end. Any footage which is captured incorrectly would be deleted upon return to base and review by management.	Risk is reduced and accepted. Mitigation of risk is proportionate to the likely impact on individuals if footage is captured incorrectly.	Policy and Procedure	
2	Inappropriate access to footage by Council Staff	Excessive processing may lead to distress of individual captured in footage	DPA Principles 1, 2 & 7	As above	Staff will only be able to access footage on the street with use of the device PIN – staff will receive training on the acceptable use of the BWV device. Parking	Risk is reduced and accepted. Mitigation of risk is proportionate to the likely impact on individuals if footage is captured	Policy, procedure, training and technical controls	

					Services Managers will be able to view recorded footage via password controlled Cloud access back office system which includes an audit log of access. Ability to download footage will be limited to CCTV Control Room staff handing the download. Downloaded materials will be securely retained and accessible on password authentication from the SSL solution. Footage exported will held in a secure area and retained in accordance with the associated policy. Access	incorrectly.		

					only provided to appropriate individuals. Training will be provided to all individuals with the chain to ensure appropriate management of footage in accordance with the associated policy and procedure.			
3	Inappropriate access to footage by members of the public	Damage and distress of the individual	DPA Principle 7	As above	As playback function is available on street staff will be trained and provided with guidance to mitigate risk of third party viewing. Any access requests for footage from members of the public will be filtered through the Subject Access Request route and relevant identification	Risk is reduced and accepted. Mitigation of risk is proportionate to the likely impact on individuals if footage is captured incorrectly.	Functionality, training and process/procedure	

					requirements.			
4	Physical security of BWV devices/ memory platform	Damage and distress of the individual	DPA Principle 7	As above	Use of password controls and encryption of technology. SSL secure site for upload of footage. AES128 is the encryption standard for footage including further two PIN protections in device.	Risk mitigated by technical solution but remains in part. Technology and security to be reviewed in association with supplier where threats or weakness in security identified with appropriate solutions	Technical and management of access controls	
5	Footage captured without consent	Possible damage and distress of the individual	DPA Principle 1	As above	Footage will be captured without consent in accordance with the relevant Sch 2&3 conditions of the Data Protection Act noted earlier in this PIA.	Accepted risk CEO to annotate reason for capture and can be used as evidence of claim for damages in relation to capture of footage	Reporting of activations and relevant decision making	
6	Risk of theft from CEO or Council premises	Damage and distress of the individual	DPA Principle 7	As above	Training to staff on personal security when completing their duties. However	Accepted risk – Council is unable to full mitigate risk of theft from	Training and technical security of devices	

					we will be unable to fully mitigate this risk if protection of equipment would affect the health and safety of the CEO. Cameras will be PIN code protected and footage encrypted using AES128 encryption to prevent access to footage held on a stolen device.	member of staff.		
7	Risk of theft from Council premises	Damage and distress of the individual	DPA Principle 7	As above	Physical security will be in place in the CEO base including access controls, display of Council ID and building security. Further security controls are in place within the Council's CCTV Control Room including signing in	Risk is reduced and accepted. Mitigation of risk is proportionate to the likely impact on individuals if footage is obtained inappropriately	Physical security procedures and related training.	

					sheets. All staff in the building should be aware of and receive regular updates of security requirements within the building.			
8	Posting of footage to social media or other area of public access	Damage and distress of the individual	DPA Principle 1, 2 & 7	As above	Those with access to footage will be trained on its appropriate use and reminded of their Data Protection requirements and the Council's Social Media Policy together with likely sanctions if data is mishandled in this way. Any inappropriate posting of footage would be a security incident and follow the appropriate	Risk is reduced and accepted. Mitigation of risk is proportionate to the likely impact on individuals if footage is captured incorrectly.	Training and associated policies	

					procedure including a request to the associated service provider to ‘take down’ the relevant footage.			

In addition to the above risks; where a security or handling complaint is received, the relevant data subject has a right to seek civil damages if they are able to demonstrate damage and/or distress. They also retain the right to approach the Office of the Information Commissioner who will review the handling of personal data and related processes and is able to impose significant monetary civil penalties.

Step 4: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	**Date for completion of actions**	**Responsibility for action**
Considerations of PIA in the final drafting of related policy and procedure within Parking Services		Parking Services
Contact for any future privacy concerns		Information Management Team and Parking Services

Step 5: Completion record for Privacy Impact Assessments

On conclusion of the project or related activity the final version of the Privacy Impact Assessment is signed to indicate completion and identifies the privacy custodian.

Role	**Name**	**Signature**	**Date**
Project Sponsor	Ben Brailsford *Parking Services Manager*		
Information Asset Owner/ Application Owner/ Privacy Custodian	Ben Brailsford *Parking Services Manager*		
Head of Information Management Team	John Curtis		

Review and assessment of the PIA

Please return your completed Privacy Impact Assessment form to the Information Management Team at: informationmanagement@sheffield.gcsx.sheffield.gov.uk

The Information Management Team will review the Assessment at any stage and assist with:

1. Identifying any additional risks and solutions which the service may not have identified.

2. Identify where there may be areas of non-compliance with statutory and regulatory requirements and any further risks that this may have on the individual or the Council.

3. Return the Assessment to you, along with any recommended changes, for acceptance of those changes and approval/sign off.

   Once the Assessment has been approved, a final approved copy should be provided to the IM Team so that this can be recorded and published (unless there are specific reasons for non-disclosure). The service will then be responsible for implementing any of the agreed solutions and actions.