Cumbria County Council Parking Services

Body Worn Video Device and Hand Held Unit Policy

1 Introduction

1.1 The Civil Enforcement Officers (CEOs) employed by Cumbria County Council, undertaking the enforcement of parking restrictions throughout Cumbria, are each equipped with a Body Worn Video Device (BWVD), which has both video and audio recording capability.

1.2 During their work, the CEOs are vulnerable to verbal and physical abuse and the Council sometimes receives complaints about the behaviour of a CEO. The BWVDs can act as a deterrent to abusive and aggressive behaviour and prevent a situation escalating and the recording can also be used as evidence in cases where a CEO is assaulted or abused. It can also be used to investigate complaints about a CEO. The BWVDs will not be used to provide evidence of parking contraventions as the handheld computer with integrated camera is used to record this evidence.

1.3 In addition CEOs are equipped with a Hand Held Unit (HHU) to issue Penalty Charge Notices which records details of vehicles including location, registration mark and photographs.

2 Legislation and Statutory Guidance

2.1 The following legislation and guidance is applicable the use of BWVDs and the HHUs:

- General Data Protection Regulation.
- Freedom of Information Act 2000.
- Human Rights Act 1998.
- Protection of Freedoms Act 2012.
- Home Office *Surveillance Camera Code of Practice.*
- Information Commissioner's Office *In the Picture: A data protection code of practice for surveillance cameras and personal information.*

2.2 General Data Protection Regulation: the Information Commissioner's Office regulates this Act and has issued guidance regarding body-worn CCTV cameras and their capture of 'personal data' and 'sensitive personal data'. Recorded images that are aimed at or may identify a particular individual is 'personal data' and this includes images and audio captured on such recording devices. The guidance makes reference to 'overt use' meaning that the equipment is not to be worn or used in a hidden or covert manner.

2.3 Freedom of Information Act 2000: this Act grants a general right of access to information held by public bodies which is not personal data. The Council's web-site details the application procedure for requests under this Act **www.cumbria.gov.uk/council-democracy/accesstoinformation/foi/Default.asp**

2.4 Human Rights Act 1998: Article 6 provides the right to a fair trial. All images captured through the use of a body-worn camera have the potential to be used in court proceedings and must be safeguarded by an audit trail in the same way as any other evidence. Article 8 of the Act concerns the right for private and family life, home and correspondence. Recordings of individuals in a public place are only public for those present at the time and may still be regarded as potentially private. Any recorded conversation between individuals should always be regarded as private and users of body-worn cameras should ensure that they refrain from recording anything which is beyond necessary with respect to a confrontational situation.

2.5 Protection of Freedoms Act 2012: Part 2 creates new regulation for, and instructs the Secretary of State to prepare a code of practice towards, closed-circuit television and automatic number plate recognition. Chapter 1 gives the full regulatory legislation of closed-circuit television and other surveillance camera technology which relates to a Code of Practice and interpretations.

2.6 *Home Office Surveillance Camera Code of Practice:* the integrity of any video data captured will be considered in accordance with this Statutory Guidance. The Home Office is the regulator for this guidance which is based around '12 Guiding Principals' which Cumbria County Council will adopt and adhere to at all times. The Council has also completed the Surveillance Camera Commissioners self assessment tool which outlines the actions taken to satisfy the '12 Guiding Principles'.

2.7 Information Commissioner's Office *In the Picture: A data protection code of practice for surveillance cameras and personal information:* this Statutory Guidance complements the Home Office Surveillance Camera Code of Practice with respect to body-worn closed-circuit television equipment.

3 Using Body Worn Video Devices and Hand Held Units

3.1 All CEOs are required to sign a *User Agreement* document to confirm they have read this policy and they agree to operate in accordance with it. The BWVDs and HHUs will be allocated to individual CEOs and the CEO must only use the BWVD and HHU allocated to them. If they need to use another BWVD or HHU this must be recorded on the *Daily Data Sheet* and a Parking Team Leader informed should the device require repair.

3.2 All BWVDs and HHUs must be signed in and out using the *Daily Data Sheet* and retained in the secure store room at their usual office base.

3.3 All BWVDs and HHUs must be securely stored when not in use. They must be fully charged before use and any recordings previously made be transferred from the device to the Council's secure server and deleted from the device at the end of each shift. The BWVDs must not be hidden and they must clearly state they are a CCTV device. They are deemed as overt devices.

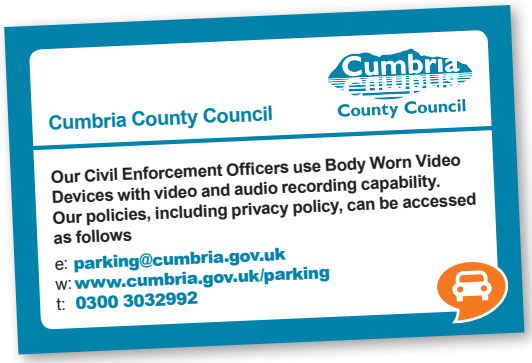
3.4 The units will not be turned on for continuous recording but can be activated at any time when the CEO feels that the behaviour of a third party is threatening or abusive. When activating the BWVD the CEO must, whenever possible, inform people that recording is taking place using a phrase such as:

"You are being recorded on video"

"Everything you say and do is being recorded"

3.5 The CEO will attempt to minimise the recording of persons present but not involved in any incident by keeping the camera focussed on the incident and not bystanders. CEOs must not intentionally fail to record incidents or obscure the camera.

3.6 The CEOs are issued with cards, as below, explaining the use of the BWVD. These are handed to customers who raise queries regarding the BWVD and advise how the Council's policies may be accessed.



4 Data Protection Considerations

4.1 Images of people are covered by the General Data Protection Regulation and a Privacy Impact Assessment has been undertaken to accompany this policy.

4.2 All recordings remain the property of Cumbria County Council but may be released to third parties in the following circumstances:-

- Requests from the police for evidence relating to criminal incidents that may have been inadvertently captured on the unit.
- Requests from the police for evidence relating to an assault on a CEO that has been reported to them by an officer of Cumbria County Council.
- Requests for footage by members of the public should be made using the council's Subject Access procedure: **www.cumbria.gov.uk/council-democracy/accesstoinformation/dataprotection/default.asp** These requests will be handled by the Information Governance Team.

4.3 Prior to releasing a copy of the recording a *Data Release Log* will be completed and the recording issued on a DVD in person to either the police or the member of the public. The Data Release Log will contain the name of the authorised officer, as below, the date of the release of the recording, the name of the person that the recording has been provided to and the reason for the release. The recording can only be released following authorisation of the Senior Manager Regulatory Services.

5 Data storage

5.1 All recordings from the BWVDs will be retained for 3 months and then deleted by the Parking Team Leader unless a recording has been flagged for retention by a Parking Team Leader or the Parking Manager. After each shift the CEO must transfer the recording from the BWVD to a secure file and following this delete the recordings from BWVD. CEOs must not delete any files or transfer any recordings to an unauthorised storage facility. The BWVDs must only be connected to a Cumbria County Council computer and not to any other computer. No files should be transferred from the computer to the BWVD. At the start of each shift the CEO must check that the BWVD contains no previously recorded footage. Failure to comply with the above may result in legal or disciplinary proceedings against the CEO. The folder is password protected and files saved can only be accessed by the Senior Manager Regulatory Services, Parking Manager and Parking Team Leaders.

5.2 Data from the HHU is automatically downloaded to the Chipside computer database at the end of each shift and the HHU automatically cleared.

6 Reporting of incidents

6.1 All incidents where the CEO has been subjected to physical or verbal abuse must be reported on an *Accident / Incident Reporting Form* or a *Safety Observation Card* or via the EOPAS/E-Safety Portal and forwarded to the CEOs Parking Team Leader who will discuss the incident with the CEO, endorse the form if necessary and forward to the Corporate Health and Safety Team for recording to ICASS. A copy of the form should also be saved onto the PCN file within the Chipside case management system and submitted to the Parking Manager.

7 Monitoring

7.1 Parking Team Leaders will carry out monthly monitoring checks to ensure that their CEOs are complying with this policy. The Parking Manager will also conduct quarterly audits to assess compliance. Any non-conformances will be immediately raised with the CEO concerned and corrective actions agreed.

7.2 Monitoring checks will be carried out in accordance with the 'Parking Services Internal Audit Plan' and recorded on the 'Parking Services Internal Audit Report' form.

General Data Protection Regulation

Privacy Impact Assessment Template

Introduction: Privacy by Design

The Information Commissioner's Office (ICO) encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

As Cumbria County Council takes its responsibilities under the General Data Protection Regulation seriously, adoption of the 'Privacy by Design' approach is essential to ensure the protection of privacy and better data protection compliance.

Unfortunately, in practice these issues are often bolted on as an after-thought or ignored altogether. Although this approach is not a requirement of the General Data Protection Regulation, it will help the council to meet its obligations under the legislation and improve customer satisfaction in relation to its data handling practices.

The ICO would like to see more organisations integrating core privacy considerations into existing project management and risk management methodologies and policies.

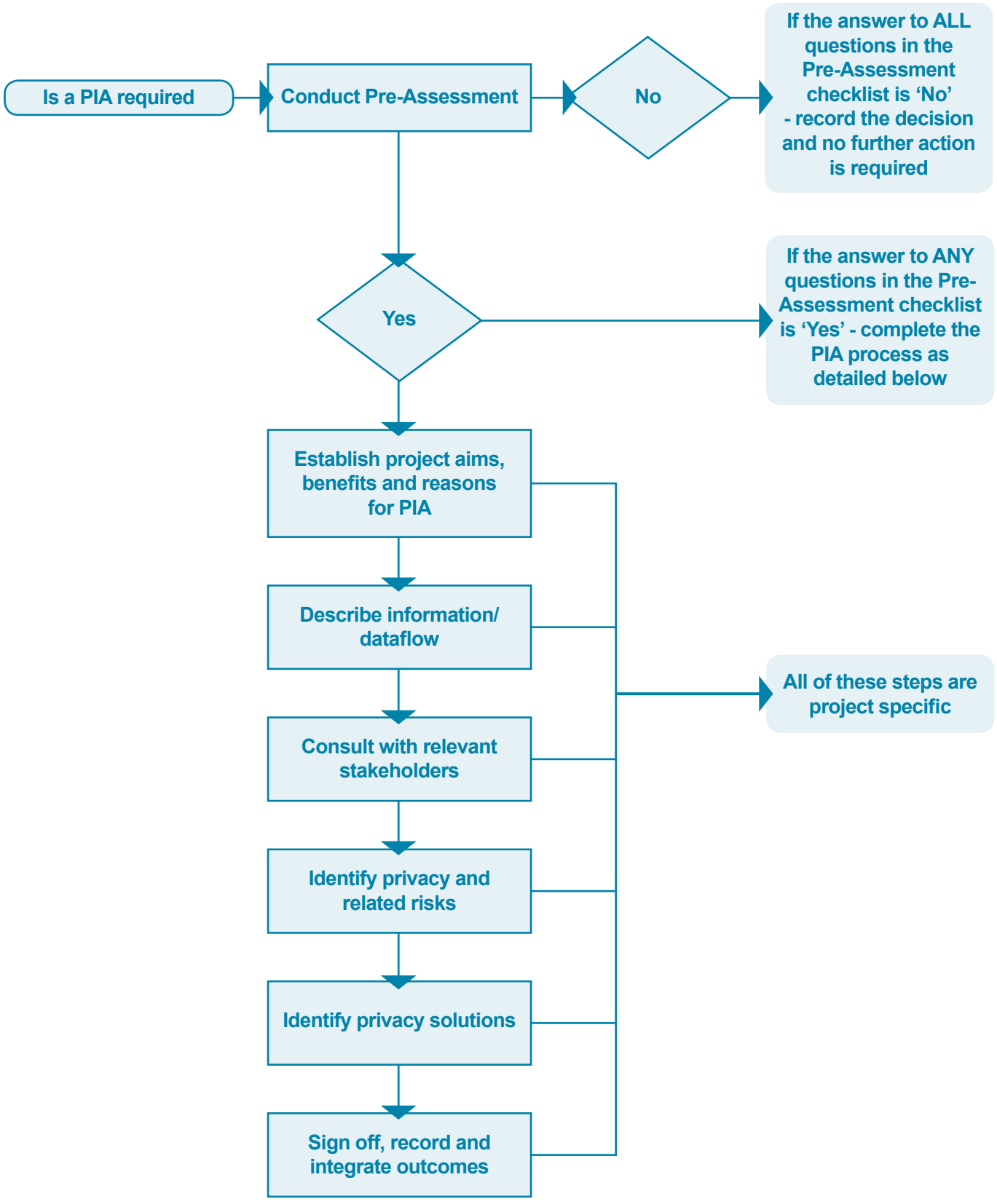
Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- potential problems are identified at an early stage, when addressing them will often be simpler and less costly;
- better awareness of privacy and data protection;
- increased likelihood of meeting legal obligations;
- reduction in potential breaches of the General Data Protection Regulation;
- actions are less likely to be privacy intrusive and have a negative impact on individuals.

Privacy Impact Assessments (PIAs) are an integral part of taking a privacy by design approach. The **Conducting Privacy Impact Assessments Code of Practice** explains the principles which form the basis for a PIA.

PIAs are a tool that can be used to identify and reduce the privacy risks of council projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help to design more efficient and effective processes for handling personal data.

Privacy Impact Assessments: Step by Step
The Privacy Impact Assessment process has the following stages:



Section 1: Pre-Assessment Checklist

These questions are designed to help you decide whether a Privacy Impact Assessment (PIA) is necessary.

Answering 'yes' to any of these questions is an indication that a PIA should be conducted. Conducting the assessment at the early stages of your project will identify privacy issues and allow discussion of relevant solutions.

Advice should always be sought from all stakeholders including Information Governance, ICT Systems/Security and Legal Services.

Screening Questions

Will the project involve the collection of new information about individuals?

Yes

Will the project ask individuals to provide information about themselves?

No

Will the project involve disclosing information about individuals to organisations to people who have not previously had routine access to the information?

Yes

Will the project use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

No

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of CCTV, biometrics or facial recognition.

Yes

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

Yes

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

Yes

Is there a privacy notice in place telling individuals about how you are going to use their data?

Yes

Is a Full Privacy Impact Assessment Required?

Yes

Section 2: Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in **Conducting Privacy Impact Assessments Code of Practice**. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Project Aims, Benefits and Reasons for PIA
This section should explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. It might also helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Aims: Privacy Impact Assessment for Civil Enforcement Officer Body Worn Video Device and Hand Held Units

Benefits: The Civil Enforcement Officers employed by Cumbria County Council, undertaking the enforcement of parking restrictions throughout Cumbria, are each equipped with a Body Worn Video Device which has both video and audio recording capability. In addition Civil Enforcement Officers are equipped with a Hand Held Unit to issue Penalty Charge Notices which records details of vehicles including location, registration mark and photographs. During their work the CEOs are vulnerable to verbal and physical abuse and the Council sometimes receives complaints about the behaviour of an Officer. The Body Worn Video Devices can act as a deterrent to abusive and aggressive behaviour and prevent a situation escalating and the recording can also be used as evidence where an Officer is assaulted or abused. It can also be used to investigate complaints about an Officer. The Body Worn Video Devices will not be used to provide evidence of parking contraventions as the Hand Held Devices are used to record this evidence.

Reasons for PIA: The documents below provide instructions for Civil Enforcement Officers when using the Body Worn Video Devices and Hand Held Units. As the Officers are working in the public domain there is a very high incidence that they will capture details of other members of the public when deploying the Body Worn Video Device and using the camera on the Hand Held Unit. As such the Body Worn Video Device may capture both video and audio of incidents not pertinent to the intended recording and the Hand Held Unit may similarly capture still images. This Privacy Impact Assessment outlines the measures Cumbria County Council takes to reduce this possibility as far as is practicably possible.

Relevant Documents:

- *Cumbria County Council Parking Services Body Worn Video Device and Hand Held Unit Policy.*
- *Cumbria County Council Parking Services Operations Manual for Civil Enforcement Officers.*
- *Cumbria County Council Privacy Policy*

Description: For data protection purposes Cumbria County Council is the Data Controller and the Data Processor in relation to any personal information being processed.

Cumbria County Council is already a notified Data Controller and Data Processor with the Information Commissioner's Office, registration number Z5623112, and the registration entry has been updated to reflect the use of the Body Worn Video Devices.

The Service's documents *Cumbria County Council Parking Services Body Worn Video Device and Hand Held Unit Policy* and *Cumbria County Council Parking Services Operations Manual for Civil Enforcement Officers* cover the use of the Body Worn Video Devices and Hand Held Units including operation, downloading images, storage, access and data retention.

All Civil Enforcement Officers are required to sign a User Agreement document to confirm they have read the Cumbria County Council Parking Services Body Worn Video Device and Hand Held Unit Policy and they agree to operate in accordance with it. The Body Worn Video Devices and Hand Held Units are allocated to individual Civil Enforcement Officers who must only use the device allocated to them. If they need to use another device this must be recorded in the Daily Data Sheet and a Parking Team Leader informed should the device require repair. At the date of issue of this Privacy Impact Assessment the Service has 29 Civil Enforcement Officers.

All devices are securely stored when not in use. They are to be fully charged before use and any recordings previously made be transferred from the device to the Council's secure server and deleted from the device at the end of each shift. The Body Worn Video Devices must not be hidden and they must clearly state they are a CCTV device. They are deemed as overt devices.

The Body Worn Video Devices will not be turned on for continuous recording but can be activated at any time when the Officer feels that the behaviour of a third party is threatening or abusive. When activating the Body Worn Video Device the Officer must, whenever possible, inform people that recording is taking place using a phrase such as "You are being recorded on video" or "Everything you say and do is being recorded".

The Officer will attempt to minimise the recording of persons present but not involved in any incident with both devices by keeping the camera focussed on the incident and not bystanders. Officers must not intentionally fail to record incidents or obscure the camera.

With respect to the Body Worn Video Device all recordings will be retained for 3 months and then deleted by the Parking Team Leader unless a recording has been flagged for retention by a Parking Team Leader or the Parking Manager. After each shift the Officer must transfer he recording from the device to a secure file and following this delete the recordings from the device. The Officer must not delete any files or transfer any recordings to an unauthorised storage facility. The devices must only be connected to a Cumbria County Council computer and not to any other computer. No files should be transferred from the Computer to the device. At the start of each shift the Officer must check that the device contains no previously recorded footage. Failure to comply with the instructions may result in legal or disciplinary proceedings against the Officer. The electronic folders are password protected and files saved can only be accessed by the Senior Manager Regulatory Services, Parking Manager and Parking Team Leaders.

With respect to the Hand Held Unit data is automatically downloaded to the Chipside computer database at the end of each shift and the HHU automatically cleared.

Consultation

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

Consultation can be used at any stage of the PIA process.

Who: Consultation will involve all officers within Cumbria County Council's Parking Services team. In addition feedback and comments from members of the public, other stakeholders and partners is welcome. Comments can be made by e-mail to **parking@cumbria.gov.uk** or by telephone **0300 303 2992 (**please note cost of calls may vary depending on mobile provider).

What: The effectiveness of this Privacy Impact Assessment will be monitored by the Parking Manager.

When: This Privacy Impact Assessment will be reviewed by the Council's Parking Manager on an annual basis or when any changes take place with respect to equipment or operational procedures.

Identification of privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Privacy Issue	Risk to Individuals	Compliance Risk	Corporate Risk
Body Worn Video Devices capture video and audio. There is a risk that the device may be stolen from the Officer.	There is a risk that images captured by the device could be circulated outside the Council's internal systems.	Potential breach of the General Data Protection Regulation.	Fines and reputational damage for the Council.
Hand Held Units capture details of parked vehicles including location, registration mark and photographs.	There is a risk that images captured by the device could be circulated outside the Council's internal systems.	Potential breach of the General Data Protection Regulation.	Fines and reputational damage for the Council.
There is a potential for both devices to capture details of third parties who are not the intended target for the recording.	There is a risk that private information relating to third parties could be captured.	Potential breach of the General Data Protection Regulation.	Fines and reputational damage for the Council

Privacy Solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution(s)	Result Is the risk eliminated, reduced, or accepted?	Evaluation Is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Inadequate disclosure controls.	Body Worn Video Device Policy and Hand Held Unit Policy and training for users.	Reduced.	Yes.
Body Worn Video Device and hand Held Unit may be seen as an unjustified intrusion of privacy.	Body Worn Video Device and Hand Held Unit Policy and training for users.	Reduced.	Yes.
Non–compliance with the General Data Protection Regulation.	Body Worn Video Device and Hand Held Unit Policy and Council's Information Security e-learning Module.	Reduced.	Yes.
Risk of the Body Worn Video Device and Hand Hend Unit being lost or stolen.	Body Worn Video Device and Hand Held Unit Policy and report to Police immediately.	Reduced.	Yes.

Sign off and record the PIA outcomes

Risk	Approved Solution	Approved By
Inadequate disclosure controls.	All users will adhere to the *Body Worn Video Device Policy and Hand Held Unit Policy*. Training will be provided for users.	Parking Manager
Body Worn Video Device and hand Held Unit may be seen as an unjustified intrusion of privacy.	All users will adhere to the *Body Worn Video Device and Hand Held Unit Policy*. Training will be provided for users.	Parking Manager
Non–compliance with the General Data Protection Regulation.	All users will adhere to the *Body Worn Video Device and Hand Held Unit Policy*. All users will complete the Council's Information Security e-learning Module.	Parking Manager
Risk of the Body Worn Video Device and Hand Hend Unit being lost or stolen.	All users will adhere to the *Body Worn Video Device and Hand Held Unit Policy*. Loss of either device must be reported to the Police immediately.	Parking Manager

Integrating 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 Required	Completion Date	Responsibility for Action
Parking Manager is responsible for ensuring that this Privacy Impact Assessment is implemented and reviewed on an annual basis or when any changes take place with respect to equipment or operational procedures.	This Privacy Impact Assessment will be reviewed on an annual basis. Reviewed: 10/05/18	Parking Manager

Contact and Further Information

Information Governance Team
Cumbria County Council
Cumbria House
107-117 Botchergate
Carlisle CA1 8RZ
t: **(01228) 221234**
e: **information.governance@cumbria.gov.uk**

CCC J/N 23670