PRIVACY IMPACT ASSESSMENT

# PRIVACY IMPACT ASSESSMENT

The template below is designed to assist you in carrying out a privacy impact assessment (PIA).

### Privacy Impact Assessment screening questions

These questions are intended to help you decide whether a PIA is necessary.

|  |  |
| --- | --- |
| Camera location (if applicable) | Body Worn Video Cameras to be used by Parking Civil Enforcement Officers |

|  |  |
| --- | --- |
| Camera Number (if known) |  |

|  |  |
| --- | --- |
| Camera type (PTZ, Static etc.) | Body Worn Video |

Is CCTV system covered by ICO registration number?  Yes  No

|  |  |
| --- | --- |
| If so, please state | Z5449999 |

Has the Surveillance Camera Code of Practice self-assessment tool been used  Yes  No  
to assist in completion of this PIA?

Will this proposed installation be part of an existing CCTV system certified to the  Yes  No  
Surveillance Camera Code of Practice?

**Checklist**

Answering ‘yes’ to any of the following questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

Introduction of a new surveillance camera system or additional camera (includes  Yes  No  
static cameras) which can collect new personal information about individuals

Changing location and/or field of view of an existing camera  Yes  No

Upgrading cameras which can obtain additional views or enhanced views which  Yes  No  
may impact on privacy e.g. HD cameras, IR lighting, more powerful lenses, 360   
degree cameras

Introduction of new technology that may affect privacy (e.g. Automatic Number  Yes  No  
Plate Recognition, Body Worn Video, Automated Recognition Technology,   
Unmanned Aerial systems (Drones) or similar

|  |  |
| --- | --- |
| If so, please state | Body Worn Video for Parking Services |

Using re-deployable cameras (to be completed for every new deployment)  Yes  No

Installation of the camera results in decisions or action against individuals in ways  Yes  No  
that can have significant impact on them (this would include, fine, notifying police,  
patching through images of suspects to police control rooms and Regulation of  
Investigatory Powers Act 2000 – RIPA)

Is the information collected about individuals of a kind likely to raise privacy  Yes  No  
concerns or expectations? For example, criminal records or other information   
that people would consider particularly private. (Note: may include radio   
transmissions from the CCTV Control room to store watch and pub watch   
systems. These regularly mention individuals and their previous convictions   
which can be heard by members of the public as well as suspect. The risk   
would need to be identified in the PIA and the solutions addressed.)

Introduction of Wi-Fi, microwave, GSM, airwave transmission etc.  Yes  No  
(Is it encrypted?)

|  |  |
| --- | --- |
| If so, please state |  |

Extending periods of recording  Yes  No

Upgrade in recording frames per second (increase in image capture)  Yes  No

Analogue to digital recording  Yes  No

Where other agencies/organisations are involved in activities where there is  Yes  No  
potential for privacy to be compromised, e.g. monitoring, handling,   
processing, sharing data/images etc.

Any alteration to the way images and data are handled, viewed, processed,  Yes  No  
disclosed, shared, disposed, retrieved, accessed, stored

Any other process or use which increases the risk to privacy  Yes  No

|  |  |
| --- | --- |
| If so, please give details |  |

Does the introduction of a camera system or individual camera increase the risks  Yes  No  
to the Organisation? E.g. potential non-compliance with data protection or other   
legislation, legal actions by individuals, etc.

If you tick ‘YES’ to any of the above, please complete the following PIA. If in doubt it would be advisable to complete a PIA anyway.

# 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.

## 1. Identify the need for a PIA

The following are examples of some of the possible aims of the installation/project. If applicable tick one or more of the following aims then briefly explain what the benefits will be to the organisation, individuals and other parties. If there are other aims please detail and explain.

You can refer to other documentation related to the proposed installation or project e.g. Operational Requirement, business case, project proposal, feasibility survey etc.

### 1.1 Aims

a. reducing the fear of crime

b. deterring and preventing crime

c. assisting in the maintenance of public order and reducing offences

d. provide high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders

e. protecting property

f. providing assistance with civil claims

g. providing assistance with issues relating to public safety and health

h. providing assistance and reassurance to the public in emergency situations

i. Assist with traffic management

j. Recognition of number plates (ANPR)

k. Other, please specify

|  |
| --- |
| Protecting the Health and Safety of Parking Civil Enforcement Officers |

### 1.2 Benefits

Having identified the aims please explain the benefits to your organisation, to individuals and to other parties. This could include such things as reduction in crime and offences, reduction in fear of crime, detection of anti-social behaviour etc. The benefits should be capable of being measured and not anecdotal (If you have completed an operational requirement (OR), as recommended, in relation to this PIA please refer to the OR for risk analysis)

|  |
| --- |
| • Reduce the number of incidents of aggressive behaviour and abuse aimed at our officers.  • Reduce protracted complaint investigations by providing impartial, accurate evidence  • Enhance opportunities for evidence capture to enable internal or police investigation following  incidents.  • Give greater insight into service delivery and identifying opportunities for improvement in the  interests of protecting the health & safety of Parking Civil Enforcement Officers |

### 1.3 Summarise why the need for a PIA was identified

Completion of the screening questions will assist in identifying the need for a PIA.

Possible needs might include:

a. Capture of new personal data/images

b. New or additional locations/areas which have potential for privacy implications

c. Use of new technology which is capable of capturing enhanced images e.g. BWV, automated recognition, 360 degree views, higher powered equipment, etc

d. Surveillance camera systems with audio recording capability e.g. BWV

e. Alteration to the way images and data are handled, viewed, processed, disclosed, shared, disposed, retrieved, accessed, stored

f. Use of technology which captures vehicle registration numbers (ANPR)

g. Other, please specify

|  |
| --- |
|  |

## 2. Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows.

### 2.1 How is information collected?

CCTV camera  BWV

ANPR  Unmanned aerial systems (drones)

Stand-alone cameras  Real time monitoring

Other (please specify)

|  |
| --- |
|  |

### 2.2 Does the systems technology enable recording?

Yes  No

Please state where the recording will be undertaken (no need to stipulate address just Local Authority CCTV Control room or on-site would suffice for stand-alone camera or BWV)

|  |
| --- |
| Body Worn Camera - on-site |

Is the recording and associated equipment secure and restricted to authorised person(s)? (Please specify, e.g. in secure control room accessed restricted to authorised personnel)

|  |
| --- |
| The equipment is secure - recordings will be encrypted, so recordings cannot be accessed, amended or deleted by unauthorised persons. Recordings from individual cameras will be downloaded to a dedicated PC used solely for this purpose in a secure area, with controlled access to the software and for viewing recordings. |

### 2.3 What type of transmission is used for the installation subject of this PIA (tick multiple options if necessary)

Fibre optic  Wireless (please specify below)

Hard wired (apart from fibre optic,  Broadband  
please specify)

Other (please specify)

|  |
| --- |
| Each camera is encrypted and downloads the recordings when the camera is connected to its local PC. These videos are stored locally on the controlled secure PC and this PC is backed up to the central server over the Councils secure network. |

### 2.4 What security features are there to protect transmission data e.g. encryption (please specify)

|  |
| --- |
| Recording is encrypted, password protected (so can only be viewed by limited authorised personnel) and can only be downloaded via a docking station and dedicated terminal housing the required software. |

### 2.5 Where will the information be collected from?

Public places (please specify)  Car parks

Buildings/premises (external)  Buildings/premises (internal public areas) (please specify)

|  |
| --- |
| Car Parks and On-Street locations by officers carrying out Parking Enforcement. |

Other (please specify)

|  |
| --- |
|  |

### 2.6 From whom/what is the information collected?

General public in monitored areas (general observation)  Vehicles

Target individuals or activities (suspicious persons/incidents)  Visitors

Other (please specify)

|  |
| --- |
|  |

### 2.7 Why is the information being collected? (Please refer to additional documentation where available)

Crime prevention and detection  Traffic control purposes

Parking enforcement  Intelligence

Missing person(s)  Other (please specify)

|  |
| --- |
| To protect the health and safety of our parking civil enforcement officers |

### 2.8 How is the information used? (tick multiple options if necessary)

Used by CCTV operators to detect and respond to unlawful activities in real time

Used by CCTV operators to track and monitor suspicious persons/activity

Used to search for vulnerable persons

Used to search for wanted persons

Used to support post incident investigation by authorised agencies, including judicial system

Used to provide intelligence for authorised agencies

Other (please specify)

|  |
| --- |
| For internal Council investigations following an incident of abuse a) to give managers insight into service delivery, which could identify training needs/ opportunities for improvement relevant to effective confict management, or b) for corroberation of evidence in investigation of complaints regarding recorded incidents of abuse. |

### 2.9 How long is footage stored? (please state retention period)

|  |
| --- |
| It will be stored for 2 months, unless identified as being required as evidence by a prosecution agency, or to assist in an internal Council investigation or relevant to a Subject Access Request. This retention period, grounds for permitted extension of this retention period, and who will have access to over-ride this extension period will form part of the Council's Body Worn Camera Policy/ Procedure. The 2 months is considered appropriate to take account of processing time allowed for Subject Access Requests. |

### 2.10 Retention Procedure

Footage automatically deleted after retention period

System operator required to initiate deletion

Under certain circumstances authorised persons may override the retention period e.g. retained for prosecution agency (please explain your procedure)

|  |
| --- |
| Authorised Council personnel will have administrative system permissions enabling them to manually over-ride the retention period for specific data requiring a longer retention period. This will be included in the Council's Body Worn Camera Policy/Procedure. |

### 2.11 With which external agencies/bodies is the information/footage shared?

Statutory prosecution agencies  Local Government agencies

Judicial system  Legal representatives

Data subjects  Other (please specify)

|  |
| --- |
| The Council's Body Worn Camera Policy/Procedure will detail who can access footage, when, how and why. |

### 2.12 How is the information disclosed to the authorised agencies

Only by onsite visiting

Copies of the footage released to those mentioned above (please specify below how released e.g. sent by post, courier, etc)

Offsite from remote server

Other (please specify)

|  |
| --- |
| Footage is held on a dedicated computer in a private Council Office.  Footage is accessible by visiting the council offices.  Where police officers require emergency access to recorded footage (for example a live ongoing incident where police officers quickly need to establish the identity of an assailant) authorised officers could divulge the encryption password to a police officer  Footage required by external agencies as identified in the policy would be released on disk/USB Recipients of information would become Data Controllers of the copy released to them. |

### 2.13 Is there a written policy specifying the following? (tick multiple boxes if applicable)

Which agencies are granted access

How information is disclosed

How information is handled

Recipients of information become Data Controllers of the copy disclosed

Are these procedures made public?  Yes  No

Are there auditing mechanisms?  Yes  No

If so, please specify what is audited (e.g., disclosure, production, accessed, handled, received, stored information)

|  |
| --- |
| The Council's internal audit team will be able to audit all aspects of use of the body worn camera systems to ensure use is in accordance with the Council's policy/procedures |

### 2.14 Do operating staff receive appropriate training to include the following?

Legislation issues

Monitoring, handling, disclosing, storage, deletion of information

Disciplinary procedures

Incident procedures

Limits on system uses

Other (please specify)

|  |
| --- |
|  |

### 2.15 Do CCTV operators receive ongoing training?

Yes  No But enforcement officers are required to review the procedure and policy annually to ensure they remain familiar with the requirements.

### 2.16 Are there appropriate signs which inform the public when they are in an area covered by surveillance camera systems?

Yes  No The cameras are very overtly worn on the outside of the uniform. The cameras have a display screen that faces the member of the public showing exactly what is being recorded, and clearly shows a bright red recording light. In addition wherever possible the officer will advise the member of the public that they have now switched their body worn audio and video camera on.

## 3. Consultation requirements

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 can use consultation at any stage of the PIA process. It will be necessary to concentrate any consultation into ‘privacy issues’.

Note: there are guidelines on consultation for the public sector issued by the Cabinet Office and elsewhere in this guidance.

### 3.1 Who have you consulted with? (tick multiple options if necessary)

**Internal Consultations**

Data Protection officer  Engineers, developers, designers, installers

Information Technology  Planning

Procurement  Data Processors

Corporate governance/Compliance  Research, analysts and statisticians

Senior management  Other (please specify)

|  |
| --- |
| CCTV Manager, Health & Safety Team, Council's Portfolio Group Holders, Civil Enforcement Officers, Union Representatives. |

**External Consultations** (tick multiple options if necessary)

General public  Local residents

Business  Education establishments

Neighbourhood panels  Other (please specify)

|  |
| --- |
| Public consultation carried out in May 2018. Published on Council's website, and promotion of this consultation via Facebook & Twitter , and article in the following newspapers : Andover Advertiser, Southampton Echo and the Romsey Advertiser |

### 3.2 How did you undertake the consultation with the above (e.g. focus groups, on-line public survey, public meetings, targeted mail survey, etc)? (please explain)

|  |
| --- |
| Online Public Consultation invited comments and feedback from the public. |

### 3.3 Is feedback available to view?

Yes  No

### 3.4 What feedback did you have and have you acted on it? (please explain or attach results)

|  |
| --- |
| There were no comments received from the public consultation.  Internal consultation - Senior Management Team and Portfolio Group were initially consulted who agreed in principal to use of the cameras, subject to a review of the cameras after one year. A Project Group was then formed consisting of representatives from the Parking Management Team, a Civil Enforcement Officer, the Senior Solicitor, an IT Manager, Internal Audit, the Health & Safety Officer and the CCTV/Community Safety Officer. In terms of the Project Group, the policy and procedures have been developed in line with the SCC Code of Practice, the ICO Code of Practice, and the Project Group's discussions. HR and the Unions were consulted.The Council's Health & Safety Officer has affirmed that the unions were consulted about the cameras during a Health & Safety meeting, and their concerns that enforcement officers need to be aware that recordings could be used for monitoring or disciplinary purposes have been addressed by including reference to this fact within the policy and procedure document. The civil enforcement officers were also consulted about their views, and any concerns about how the cameras should be used have been addressed within the policy and procedures. The policy and procedure was developed in response to the views of all of these parties.The Council's Policy and Procedure Review Group have approved the final policy and procedure. All officers using the equipment are required to read this document as part of the training, and sign to confirm that they have read, understood and will comply with the procedures. |

## 4. Identify the privacy and related risks

**Below are some suggested risks and solutions. Feel free to use some or all of them or some of your own.**

The below table provides some examples of possible privacy risks related to the use of a CCTV system. Operators can use this list as a starting point; however, not all of these risks may apply to all CCTV systems or all PIAs.

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. Remember that the aim of a PIA is not to completely eliminate the impact on a privacy risk. The options in dealing with the risks are to eliminate, reduce or simply accept them.

| **Privacy issue** | **Risk to individuals** | **Compliance risk** | **Associated organisation / corporate risk** |
| --- | --- | --- | --- |
| Collection of Data | Contravention of an individual's privacy rights.  Unauthorised access to data. | Non-compliance with Data Protection Act 1998 - contravenes Principle 1 (Fair & Lawful Processing) &  Human Rights legislation | Claims for compensation, fines and sanctions.  Loss of reputation. |
| Loss or Misuse of Data | Footage being kept for longer than necessary.  Unauthorised access to data.  Full Audit Trail not available.  Data being used for a purpose other than intended. | Non-compliance with GDPR 2016 and DPA 2018, and human rights legislation. | Claims for compensation, fines and sanctions.  Loss of reputation. |
| Footage being retained un-necessarily | Information might be used for longer than necessary, if a retention period has not been establised. | Non-compliance with GDPR 2016 and DPA 2018, and human rights legislation. | Claims for compensation, fines and sanctions.  Loss of reputation. |
| Images recorded in private as opposed to public areas | Misuse of footage | Non-compliance with , Human Rights Act 1998 - contravenes Article 8 (the right to respect for private and family life, home and correspondence) | Claims for compensation, fines and sanctions.  Loss of reputation. |
| The use of images in court proceedings | Measures being taken against individuals as a result of collecting information about them might be seen as intrusive | Non compliance with Human Rights Act 1998 - contravenes Article 6 (the right to a fair trial) | Claims for compensation.  Loss of reputation. |
| Potential for Covert Surveillance | Contravention of Privacy Rights | Regulation of Investigatory Powers Act (RIPA) 2000 | Claims for compensation, fines and sanctions.  Loss of reputation. |

## 5. Identify 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).

Note: please mark any ‘privacy by design’ solutions with an asterisk \*

| **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? |
| --- | --- | --- | --- |
| Collection / use / loss of data | Data only to be collected for the specified purpose(s) for which it was introduced as detailed in the Council's policy/procedure. If an error is made eg Officer forgets to switch camera off when an incident ends, erroneous footage can be deleted by authorised Council administrator \*  Recordings are encrypted, password protected and can only be downloaded via a docking station and viewed on a dedicated PC.\*  Access to data on a secure server, on a dedicated PC and available only to specified individuals, as identified in the Council's BWV Policy. \*  All data passed to authorised external agencies to be signed for by the person receiving the data, and they become the data controller.  A privacy notice will be on the Council's website so that the public are informed what data is being collected, the purpose, how it will be stored, retained, accessed.. | Reduced | Final impact deemed justified, compliant and proportionate to project aims. |
| Un-necessary retention of images/information | The system will be set to retain data for a specified retention period (2 months) except in limited circumstances as specified in the Councils BWV Policy & Procedures. This retention period will be included within the Council's Retention schedules, and a Privacy Notice on the Council's website will detail this retention policy. | Reduced | Retention periods will be introduced (60 days) which is deemed justified, compliant and proportionate |
| Images recorded in private as opposed to public areas | All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, practical use eg when to commence and cease recording, and health and safety. Written procedures will also be in place.  In the unlikely event of any unauthorised use of cameras, this will be captured, and any attempt to delete recordings will be logged on the BWC audit  trail. Recordings will be subject to audit to ensure compliance.  Relevant policies will put in place as stated, and training in place for users and processors.  Checks will be carried out to ensure compliance. | Reduced | This is deemed justified, compliant and proportionate |
| The use of images in court proceedings | All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, practical use eg when it is appropriate to record and when to commence and cease recording, and health and safety. | Reduced | Impact deemed justified, compliant and proportionate |
| The potential for covert surveillance | BWV will only be deployed in an overt manner. This will be stated in the Council's BWV Policy. The public will be aware of the Overt Surveilliance as Enforcement Officers using the BWCs will wear the cameras overtly on the outside of their uniforms. The procedures will also require staff to inform the public that they are being recorded on video and audio. Procedures and training in place. Checks will be carried out to ensure compliance | Reduced | Impact deemed justified, compliant and proportionate |

## 6. Sign off and record the PIA outcomes

This section is for the decision maker in the organisation to sign off each risk. Who has approved the privacy risks involved in the project; what solutions need to be implemented; who and at what level?

The example below shows the information required. You will need to list each identified risk, solution and approved sign off.

| **Risk** | **Approved solution** | **Approved by** |
| --- | --- | --- |
| Collections / use / loss of data | Data only to be collected for the specified purpose(s) for which it was introduced as detailed in the Council's policy/procedure. If an error is made eg Officer forgets to switch camera off when an incident ends, erroneous footage can be deleted by authorised Council administrator \*  Recordings are encrypted, password protected and can only be downloaded via a docking station and viewed on a dedicated PC.\*  Access to data on a secure server, on a standalone PC and available only to specified individuals, as identified in the Council's BWV Policy. \*  All data passed to authorised external agencies to be signed for by the person receiving the data, and they become the data controller.  A privacy notice will be on the Council's website so that the public are informed what data is being collected, the purpose, how it will be stored, retained, accessed. |  |
| Un-necessary retention of images/information | The system will be set to retain data for a specified retention period (2 months) except in limited circumstances as specified in the Councils BWV Policy & Procedures. This retention period will be included within the Council's Retention schedules, and a Privacy Notice on the Council's website will detail this retention policy. |  |
| Images recorded in private as opposed to public areas | All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, practical use eg when to commence and cease recording, and health and safety. Written procedures will also be in place.  In the unlikely event of any unauthorised use of cameras, this will be captured, and any attempt to delete recordings will be logged on the BWC audit  trail. Recordings will be subject to audit to ensure compliance.  Relevant policies will put in place as stated, and training in place for users and processors.  Checks will be carried out to ensure compliance. |  |
| The use of images in court proceedings | All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, practical use eg when it is appropriate to record and when to commence and cease recording, and health and safety. |  |
| The potential for covert surveillance | BWV will only be deployed in an overt manner. This will be stated in the Council's BWV Policy. The public will be aware of the Overt Surveilliance as Enforcement Officers using the BWCs will wear the cameras overtly on the outside of their uniforms. The procedures will also require staff to inform the public that they are being recorded on video and audio. Procedures and training in place. Checks will be carried out to ensure compliance |  |