

	Stoke-on-Trent City Council
	BODY WORN VIDEO CAMERA



ANNEX 2

BODY WORN VIDEO CAMERA

Contents

1. Introduction and Scope	3
2. Legislative Framework	4
3. General Principles of Operation	4
4. Accountability.....	5
5. Maintenance	5
6. Data Storage.....	6
7. Access to Data	6
8. Privacy	7
9. Accessing Images.....	7
10. Subject Access Requests	8
Appendix 1 – Local Operating Procedures for Civil Enforcement Officers	9
Appendix 2 – Local Operating Procedures for Public Protection Officers	17

1. Introduction and Scope

- 1.1 This policy sets out Stoke-on-Trent City Council's ("the Council") protocol and procedure for Body Worn Video ("BWV") devices worn by its officers.
- 1.2 It has been drafted to promote public confidence by developing a safe and secure environment for members of the public and Council officers.
- 1.3 This policy has a dual purpose, in that it will assist operators and other staff involved in the use of body worn video to understand their obligations whilst reassuring the public that appropriate safeguards exist.
- 1.4 This policy will ensure staff comply with the relevant legislation relating to surveillance cameras and personal information and outline the benefits to staff and the general public. Detailed procedures will explain how the Council will maintain the integrity of the data, images and video collected along with data security and its use.
- 1.5 BWV devices will be used to gather evidence in respect of the investigation of any offence or suspected offence for both internal and external investigations and can also act as a deterrent to acts of aggression and verbal / physical abuse towards Council officers.
- 1.6 The BWV device is issued to Council officers as part of their Personal Protective Equipment in line with their Risk Assessment as a method of mitigating potential abuse to the officers. The BWV device will be clearly worn by the officer in an overt manner and the device will clearly show that it is a CCTV recording device by either signage or verbal instruction as appropriate.
- 1.7 For the purpose of the scheme, the Council is the Data Controller. The Council is registered with the Information Commissioner's Office, Registration Number: Z5110678.
- 1.8 Across the Council, there are a number of different Council officers which utilise BWV. These are:-
 - Civil Enforcement Officers (as set out at Appendix 1)
 - Public Protection Officers (as set out at Appendix 2)

2. Legislative Framework

2.1 The BWV system will be operated in compliance with the following legislation and statutory guidance:

- Data Protection Laws¹
- Freedom of Information Act 2000
- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Home office Surveillance Camera Code of Practice (the SC Code)
- Information Commissioner's CCTV Code of Practice (the ICO Code)
- Criminal Procedures and Investigations Act 1996

3. General Principles of Operation

3.1 The following principles of operation apply to all uses of BWV across the Council. In addition, local operating procedures specific to individual departments are set out within the appendices to this policy.

- Prior to its installation and use, a camera system must have a clearly defined purpose which is in pursuit of a legitimate aim and it must be necessary to meet an identified pressing need. It should only be used for the specific purpose which it is established to address.
- Therefore, prior to use of BWV, a Data Protection Impact Assessment will be undertaken in compliance with the SC Code and the ICO Code. It should take into account the nature of the problem the proposed system is seeking to address, whether a surveillance system is justified and effective, whether better solutions exist, what effect its use may have on individuals and whether, in light of this, its use is a proportionate response. It is accepted that body worn video cameras (BWV) are more intrusive than normal CCTV because of their mobility and the level of intrusiveness must be taken into account as part of the Data Protection Impact Assessment.
- Carrying out a Data Protection Impact Assessment ensures that the system is justifiable and there is consultation with those most likely to be affected with appropriate safeguards for the impact on their privacy. This also demonstrates that the necessity and extent of any interference with Article 8 of the Human Rights Act 1998 has been considered.
- Where the BWV utilises audio then, in addition to the capturing images, the use of audio also needs to be justifiable as this adds to the privacy intrusion.
- Where it is intended to use BWV in more sensitive areas e.g. private dwellings, schools, care homes, there will need to be a pressing social or investigative need which will have to be far greater in order for the use of BWV to be necessary and proportionate. In the case of civil enforcement, an additional DPIA should be carried out to demonstrate that this is the case.

¹ means the Data Protection Act 2018 or any successor legislation and (for so long as and to the extent that the law of the European Union has legal effect in the UK) the General Data Protection Regulation ((EU) 2016/679) and any other directly applicable European Union regulation relating to privacy.

- Continuous recording requires strong justification as it will capture people going about their daily business as well as the individual who is the focus of attention.
- BWV should have robust technical and physical security in place to protect the recorded information. Devices must be capable of being encrypted and should have the ability to be turned on or off, with features to allow image and sound recording separately.
- Clear signage must be displayed, for example on an individual's uniform, to show that recording is taking place and whether the recording includes audio.
- BWV will only be used by trained, authorised personnel.

4. Accountability

4.1 It is a recommendation of the Surveillance Camera Commissioner and the Information Commissioner that the system should be reviewed annually to determine whether BWV continues to be justified. As such, there will be an annual review of the Council's use of BWV covering the following aspects:

- a) ensuring the BWV remain necessary, proportionate and effective in meeting their stated purpose for deployment
- b) whether the purpose and objectives statements remain valid
- c) change in extent of the scheme
- d) contracts with suppliers e.g. maintenance agreements
- e) a review of the data protection or legal requirements
- f) maintenance schedule and performance test of the system
- g) scheme evaluation findings
- h) complaints procedure and evaluation

As part of the annual review of the scheme, there will also be an annual review of this policy. In addition, the policy will be kept up to date with changes in legislation and procedure as and when they occur. The officer responsible for updating this policy is the Parking Group Manager.

5. Maintenance

- 5.1 Equipment must be kept in good working order. The BWV devices must be checked they are working correctly at the start of the shift or operation and any faults reported immediately to the on duty supervisor or camera librarian (or nominated deputy). It is the responsibility of each user to report any faults or damage to the on duty supervisor or nominated deputy during their shift or at the end of the shift. A log in the Council officer's pocket notebook must also be made should there be a break in a recording due to a technical failure.
- 5.2 There may be other reasons where an incident is only partially recorded, such as through the equipment being knocked, covered or dislodged during a struggle or through the nature of the incident where the camera view is restricted. There may also be occasions where the sound recording is unclear or verbal responses are difficult to hear because of other more prominent

sounds such as traffic or noise created by strong winds. In this case, the Council officer is to make notes as necessary to support any BWV device evidence.

- 5.3 In order to ensure that clear images are recorded at all times the equipment for making recordings and any associated security equipment will be maintained in good working order with regular servicing in accordance with the manufacturer's instructions. In the event of a malfunction the equipment will be repaired within specific time scales which will be scheduled within the maintenance agreement. All documentation relating to the equipment and its servicing and malfunction is retained and will be available for inspection and audit.

6. Data Storage

- 6.1 All footage will be uploaded automatically, once the BWV device has been docked on the docking station, to the BWV device software.
- 6.2 If any incidents have occurred during the shift it is essential that officers complete a '*Report of Incident / Injury / Near Miss*' report form, including the time and location of the incident. The report must also indicate if the police have been involved. Once an incident has been received a clip of the incident will be created by an authorised officer and saved on the secure server. Data storage for public protection purposes will be in accordance with retention requirements in the CPIA and ACPO Good Practice Guide for Digital Evidence.

7. Access to Data

- 7.1 Where BWV is used, a register or Digital Evidence Management System will be kept to show the life of the recorded media at all stages whilst in the Council's possession. Such a register may also show itself to be useful in enabling evaluation of the BWV scheme.
- 7.2 The register should include the following:
- unique equipment reference number(s);
 - time/date/person removing medium from secure storage for use;
 - time/date/person returning medium to secure storage after use;
 - remarks column to cover additional points (e.g., erase/destroy/handed over to law enforcement agencies/removed from recording machine);
 - time and date of delivery to the law enforcement agencies, identifying the law
 - enforcement agency officer concerned;
 - in the event of a non-automated system of erasure of data, the time/date/person responsible for erasure and/or destruction.
 - Details of all reviews of images, including persons present, purpose, date/time and results.

- 7.3 Each department utilising BWV will have their own retention periods and these are set out in the local operating procedures attached as appendices to this policy.

8. Privacy

- 8.1 Recordings from a BWV device provide an account of what the officer saw and heard during an incident. There are however limitations to the technology and wearers must be aware that some aspects of incidents vital to the evidence for the incident may occur out of camera view, that sound recordings may not be complete or that other sounds at the scene may block significant statements by those present. There is the possibility of other technical failures or operator errors that may hinder the production of the recorded evidence. Officers need to ensure that they remain mindful of standard evidence gathering procedures at scenes and must not rely solely on the BWV evidence to support their incident.
- 8.2 There are situations where the use of BWV Devices is not appropriate; the following list is for guidance only and is not exhaustive.
- **Intimacy** – BWV must not under any circumstances be used for the recording of intimate circumstances where persons are in a state of undress.
 - **Legal privilege** – users must be careful to respect legal privilege and must not record material that is or is likely to be subject to such protections.
 - **Private dwellings** – users must consider the right to private and family life.

9. Accessing Images

- 9.1 Requests to view files may be received from the following third parties (but not limited to):
- The Police
 - Solicitors
 - Claimants in Civil Proceedings
 - Accused Persons or Defendants in criminal proceedings
- 9.2 Reasons for requests may include (but not limited to):
- Evidence in criminal proceedings
 - Evidence in civil proceedings or tribunals
 - The prevention of crime
 - The investigation and detection of crime, which may include the identification of offenders
 - The identification of witnesses
 - Complaints made against Council officers
 - Complaints made against members of the public

9.3 If a third party requests access to images they must provide any details that the Council require to substantiate the request. A log of all requests will be made.

9.4 To make a request for information, a request should be made in writing to:

Information Rights Team
Civic Centre
Glebe Street
Stoke on Trent
ST4 1HH
Or email: foi@stoke.gov.uk

10. Subject Access Requests

10.1 Any individual (employee or member of the public) may request access to and a copy of their own image under Data Protection Laws.

10.2 To make a request for information, an individual should contact:

Information Rights Team
Civic Centre
Glebe Street
Stoke on Trent
ST4 1HH

Email: foi@stoke.gov.uk
Tel: 01782 235965

10.3 Any footage required as part of an internal investigation must be approved by Information Assurance and cleared by HR. Footage will then be burnt to a disc and kept in a secure location for the duration of the investigation until which time it will be destroyed.

Appendix 1 – Local Operating Procedures for Civil Enforcement Officers

This appendix sets out procedures which are specifically relevant to BWV utilised by Civil Enforcement Officers (“CEO”). The use of BWV by Civil Enforcement Officers will comply with this policy and also the details set out in this appendix and its annexes.

1. Scope

Stoke-on-Trent City Council (“the Council”) is responsible for the delivery of parking enforcement to the County of Staffordshire. Enforcement is carried out on behalf of Staffordshire County Council, Staffordshire Moorlands District Council, Cannock Chase District Council, Tamworth Borough Council, Lichfield District Council, South Staffs District Council and East Staffs Borough Council.

The BWV device will not be used to gather evidence to support Penalty Charge Notices issued by the CEOs, but may be used if a complaint is made against a CEO’s conduct.

2. Operational Guidance for CEOs

2.1 Training

All CEOs will receive full training in the use of the Body Worn Video devices. The training will include operational guidance and use of the equipment. The CEOs are trained to City and Guilds Level 2 in parking Enforcement standards, which includes *Level 2 Principles of conflict management in parking enforcement* and *Level 2 Roles and responsibilities of Civil Enforcement Officers*. There will also be on-going refresher training in conflict management.

2.2 Daily Use

The BWV device will record the entire shift of the CEO. This is to capture any acts of aggression aimed at the officers that are not directly linked to the issuing of a Penalty Charge Notice.

The CEO MUST inform any members of the public that the device is recording with a clear verbal instruction before any conversation takes place. There are no set words given to the officers to say but it should be clear, plain, easily understood speech. An example of which is:

“Sir / Madam, in line with our protocols I must advise you that this conversation is being recorded”

Recordings will not be used to gather evidence in relation to a parking contravention, but may be used to support any complaints made against the CEO.

All CEOs will be issued with a BWV device by the on – duty supervisor or nominated deputy. The CEO will ensure the unit is in full working order. The CEO will affix the

BWV device to their uniform and ensure the camera angle is correct. Once the CEO begins their patrol, the CEO will commence recording and identify themselves for the benefit of the recording, including their name, collar ID, date, the time they are on duty and the areas they are patrolling. Comfort / meal breaks will not be recorded. Breaks in recording will be traceable through the CEO Activity Report where a CEOs location and meal breaks and other activities are recorded.

The BWV devices are not being used to monitor the Civil Enforcement Officers. However if during the review of evidence poor Health and Safety practices or acts of misconduct are observed then under the statutory duty of care prescribed in Health and Safety at Work Act 1974, the department manager will be informed.

If a CEO attends an incident and is recording evidence using a BWV device, the whole incident should, where practicable, be recorded. CEOs must not intentionally fail to record an incident by, for example, turning away without good cause or deliberately obstructing the camera lens. Such calculated actions may render the BWV user to a misconduct investigation.

2.3 End of Shift

The BWV devices will be placed in their docking stations for footage download and charging.

The BWV device is encrypted, ensuring that viewing of the footage can only be carried out by an authorised officer. The duty supervisor or nominated deputy should ensure the issue and returns log is available to show evidential continuity if required. As set out above in the main body of the policy, the Council is required to have regard to the 12 guiding principles from the Surveillance Camera Code of Practice. The principles are replicated below and each principle is accompanied by a description of how the use of BWV by Civil Enforcement Officers operates in accordance with the corresponding principle.

- 1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.**

BWV devices are utilised as an improvement to the health and safety of our CEOs. Since our partnership with Staffordshire County Council our officers are working in more remote areas further away from our depots and there have been 19 incident reports in the north of the county and 4 in the south for the period July to September 2015.

Incidents reported by our CEOs are often unrelated to their civil enforcement activity and come without warning. To this end it is the decision of this authority to record the CEOs entire shift and not just individual incidents.

- 2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.**

The BWV devices will be worn on the CEOs uniform in an overt manner. Wherever possible the officer will issue a verbal instruction that recording is taking place. There is an LED on the badge to indicate recording is taking place. Footage will only be viewed if an incident has been reported, either by the officer or other third parties or if a complaint is made regarding the conduct of the officer.

3. **There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.**

Any requests to view footage should be made to:

Information Rights Team
Civic Centre
Glebe Street
Stoke on Trent
ST4 1HH

Or email: foi@stoke.gov.uk

Any complaints regarding the conduct of an officer should be made, within 28 days of the incident, to:

Customer Feedback Team
Floor 2
Civic Centre
Stoke-on-Trent
ST4 1HH

Or email: customer.feedback@stoke.gov.uk

4. **There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.**

The system is password protected and all footage is held and controlled within a secure, encrypted software package.

All passwords are unique and users access will be deleted if officers leave the authority or change posts.

5. **Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.**

Access to the protocol and procedures document will be available to all officers, along with operation guidance from the BWV device supplier. Training is available from the supplier and in – house.

6. **No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.**

Images will be kept for 28 days before deletion by the software unless required. If required by a third party a copy of the images will be burned to a DVD and handed to the person requesting the information should their request be approved. If the images are required for an internal investigation a copy of the images will be burned to a DVD and stored in a secure place. They will then be destroyed no longer than 28 days after the completion of the investigation.

7. **Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.**

Access to images is limited to those listed in Annex 1

8. **Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.**

The Council will pro – actively monitor industry advancements and adopt these accordingly.

The use of this technology will be discussed with our partners within the Midlands Service Improvement Group (MSIG) to ensure best practice.

9. **Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.**

Access to the system is limited to the officers listed in Annex 1. All users have unique passwords that will be deleted if officers leave the authority or change posts. All authorised officers have attended Data Protection training.

10. **There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.**

The system will be reviewed by the Council's audit department to ensure compliance with local and national guidelines.

The cameras will be issued to staff as part of their Personal Protective Equipment, as stipulated within the Risk Assessment for '*Duties relating to the role of Civil Enforcement Officer*'.

Training and guidance notes will be given to all CEOs and the training will be documented on a training matrix.

11. **When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.**

A tendering exercise was carried out to determine the best supplier for this technology and it was decided that *Edesix* could provide the best product for our needs.

The Council have decided to record the full CEO shift in order to fully support the health and safety of its officers and also ensure evidence is available to support any queries or complaints from the public.

Recording the complete shift will protect the CEO's and members of the public from any potential wrongdoing.

Incidents of aggression towards CEOs employed by the Council are frequent. Across the Operation Division during the period of July to September 2015, there were a number of incidents reported to the Health and Safety team.

12. **Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.**

The '*Report of Incident / Injury / Near Miss*' report form will be used to document an incident and also reference any footage gathered by the BWV device. These reports are logged by our Health and Safety team and reported on divisionally and corporately.

Annex 1 – Roles and Responsibilities

Responsible Officer	Responsibilities
Assistant Director – Governance (Monitoring Officer)	<p>For the purpose of this policy, the Council's Senior Responsible Officer is the Assistant Director – Governance (Monitoring Officer).</p> <p>The role of the SRO is to deliver a corporate approach to the Council's responsibilities arising from the Protection of Freedoms Act 2012. The SRO has strategic responsibility for the integrity and efficacy of the processes in place within the local authority which ensure compliance with section 33 of the Protection of Freedoms Act 2012 and in respect of all relevant surveillance camera systems operated by the Council.</p>
Parking Group Manager	<p>System Manager. Receiving, review and authorising or rejecting Subject Data Access forms. Viewing of Saved files</p>
Enforcement Manager (North) /Operations Manager/Contract Manager	<p>Downloading and copying of images. To act as System Manager in the absence of the Team Manager – Parking. Investigating actual or suspected breaches of Health and Safety practice or acts of misconduct in accordance with relevant council policy. System checks. Viewing of saved files.</p>
Civil Enforcement Officer – Supervisor	<p>Under the instruction of the Civil Enforcement Service Lead / Contract Manager, downloading of images. Viewing of saved files for training purposes.</p>
Strategic Manager – Enforcement and Operations	<p>Viewing of saved files.</p>

Annex 2 - Evidence Request Form

Date: _____

Details below relate to an incident recorded via a Body Worn Video Device and downloaded to CD for the purpose of Police / Incident / Internal Investigation.

Date: _____

Time: _____

Details of Incident:

The CD has been handed to: _____

Crime Ref / Log No: _____

Ref No: _____

Date: _____

Received By: _____ Signed: _____

Delivered / Handed by: _____ Signed: _____

Annex 3 – Body Worn Video Device Data Access Log

Appendix 3



City of
Stoke-on-Trent

Body Worn Video Device Data Access Log

[illegible]

Appendix 2 – Local Operating Procedures for Public Protection Officers

This appendix sets out procedures which are specifically relevant to BWV utilised by Officers from the Council's Public Protection Service. The use of BWV by these Officers will comply with the policy together with the details set out in this appendix and its annexes.

1. Scope

Stoke-on-Trent City Council ("the Council") is responsible for the delivery of a range of regulatory functions across the City of Stoke-on-Trent. These include (but are not limited to) Trading Standards, Environmental Health and Licensing functions. The use of BWV devices will be used where necessary and proportionate to gather evidence during investigations, to further enquiries in those investigations and to protect officers and members of the public from aggressive or otherwise inappropriate behaviour and malicious complaints.

2. Operational Procedures for Public Protection Officers

2.1 Training

Service managers will nominate officers to be authorised to use BWVs. These officers will receive full training in the use of the Body Worn Video devices. The training will include operational guidance and use of the equipment. Two officers will be designated as "Camera Librarians (CL)" and will receive additional training in the allocation and maintenance of the cameras and in the retrieval of data from those devices.

2.2 Operational Use – Pre deployment

The Council's Public Protection Service uses the Digital Evidence Management System (DEMS) software system to manage its BWVs. DEMs will be set such that non-evidential recordings are deleted after 28 days.

On receipt of a new camera a CL will register it onto the DEMS system. The CLs are responsible for maintaining the cameras and for ensuring they are at operational readiness at all times.

Before deploying a camera the lead officer for an operation or visit will complete an authorisation form (at Annex 2) which must be signed by a Service Manager or Lead Officer who must be satisfied that the camera's use is necessary and proportionate in all the circumstances.

Once a camera's use is approved the CL will issue officers with a camera and record that issue on the DEMS system. The CLs will keep a stock of formatted SD cards in a secure location and where issuing RS2 cameras will also issue an SD card to the officer.

2.3 Deployment

On arrival at the intended location authorised officers will activate record on the camera and bookmark the recording in accordance with national guidelines. All officers deployed on an operation with a BWV must activate their camera and it must operate throughout the operation. Any break in recording because of technical failure or for operational reasons such as the presence of children must be bookmarked on camera and be recorded in the officers pocket book.

Officers will provide an oral warning that they are recording sound and vision upon entering the premises and refresh that warning as appropriate.

The officer in charge at a premises will have regard to the Criminal Investigations and Procedures Act 1996 and the decision in R V Birmingham 1992 and ensure all recorded material is retained.

The BWV devices used by Public Protection Officers are devices “authorised” to be used to interview suspects as defined by paragraph 1.6(a) of Code of Practice E of the Police and Criminal Evidence Act 1984.

2.4 Post Deployment

On return to base after an operation the camera (and where appropriate the SD) will be handed to the CL. The CL will ensure the footage is uploaded to the DEMS system and where required marked as evidential material. The CL will then format any SD card or ensure all data is removed from the camera itself.

To comply with ACPO guidelines on the production of digital evidence the CL will then produce two copies of the footage on WORM media. One will be sealed in an evidence bag, given an exhibit number and stored as the CLs exhibit. The other will be provided to the officer in charge of the operation as a working copy.

The working copy will be treated as part of the case materials and will be stored and handled securely and in line data protection guidelines and evidential procedures.

2.5 Any requests to view footage are to be made to:

Information Rights Team
Civic Centre
Glebe Street
Stoke on Trent
ST4 1HH
Or email: foi@stoke.gov.uk

The CL will be responsible for producing copies of footage where requested after approval has been received by the relevant Service Manager.

Annex 1 – Roles and Responsibilities

Responsible Officer	Responsibilities
Assistant Director – Governance (Monitoring Officer)	<p>For the purpose of this policy, the Council's Senior Responsible Officer (SRO) is the Assistant Director – Governance (Monitoring Officer).</p> <p>The role of the SRO is to deliver a corporate approach to the Council's responsibilities arising from the Protection of Freedoms Act 2012. The SRO has strategic responsibility for the integrity and efficacy of the processes in place within the local authority which ensure compliance with section 33 of the Protection of Freedoms Act 2012 and in respect of all relevant surveillance camera systems operated by the Council.</p>
Service Manager	<p>Responsible for nominating officers to be authorised to use cameras and officers to act as Camera Librarians.</p> <p>Ensuring appropriate training is provided and equipment is maintained.</p> <p>Approving the use of cameras for a given visit or operation.</p>
Lead Officer	<p>Approving the use of cameras for a given visit or operation.</p>
Camera Librarian	<p>Maintenance & issue of equipment. Production of copies of footage Production of footage as an exhibit</p>
Officer in Charge of Investigation/Disclosure Officer	<p>Viewing of files & use in the investigation Security & Use of Working Copies. Compliance with the CPIA.</p>

Annex 2 – Human Rights Act 1998 Assessment Form

OFFICIAL SENSITIVE



City of

Stoke-on-Trent

Human Rights Act 1998 Assessment Form

This form should be completed where a pre-planned activity is being considered that will, or is likely to, breach a person's rights under the Human Rights Act 1998 and where there is no other statutory regime that puts safeguards in place. For example the conduct for covert surveillance is governed by the Regulation of Investigatory Powers Act 2000 and any such activity must be authorised under that regime.

1) Applicant's Name		3) Unique Reference Number	
2) Office, Rank or Position		4) Operation Name (if applicable)	

5) Statutory Purpose

Describe duties you are tasked to undertake on behalf of the authority that gives the authority a right to breach the subjects' Human Rights *Describe what function you are carrying out. For example this maybe the prevention or detection of crime, the apprehension of offenders, the protection of public health or safety or the protection of the legitimate rights of others.*

6) BACKGROUND DETAIL (The When, the What, the Who and the How)

Describe activity you wish to undertake and the background information that has led to your decision to undertake that activity. *Describe the activity you wish to undertake, who is that activity is directed against and what the background to the case is that had led you to decide to carry out that activity.*

7) NECESSITY (The Why – part 1)

State the nature of the investigation or operation and how it relates to a purpose at question 5 *Give a short explanation of the crime (or other purpose), the suspect, victim or witness and the activity and you wish to undertake and how all these three link together.*

8) PROPORTIONALITY (The Why – part 2)

State why the activity is proportionate to what you are seeking to achieve

Outline what is expected to be achieved from the information gathered during the activity and explain how the level of intrusion is justified when taking into consideration the benefit the information will give to the investigation. When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy? Consider other statutory regimes and state why they do not apply.

9) COLLATERAL INTRUSION

Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances

If you have identified any meaningful degree of collateral intrusion, explain what it is.

10) REGULATION OF INVESTIGATORY POWERS ACT 2000, INVESTIGATORY POWERS ACT 2018

The form is for activities that fall outside the scope of this legislation. Justify why this legislation does not apply and identify any planned or potential onward activity that may later fall under this legislation.

11) APPLICANT

Applicant's Signature

Date

12. AUTHORISING OFFICER. This should normally be a service manager within the Public Protection Service. Where no service manager is available a lead officer can approve the activity. Reasons why no service manager is available should be recorded.

The authorising officer considers the application and if approved records their considerations:

- Why do you **believe** the activity is necessary for the statutory function identified
- Why do you **believe** the conduct involved is proportionate to the objective(s)? If the applicant has identified any meaningful degree of collateral intrusion, why you **believe** the request remains justified and proportionate to the objective(s)?
- Balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explain how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- Consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Consider any statutory regime that might be relevant and state why it does not apply.

My considerations in approving / not approving this application are:

Name

Office, Rank or Position

Signature

Time and Date