PENDLE BOROUGH COUNCIL

CORPORATE POLICY

FOR THE USE OF

COVERT SURVEILLANCE

AND

COVERT HUMAN INTELLIGENCE SOURCES

TO COMPLY WITH THE PROVISIONS OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

REVISED JULY 2020

CONTENTS

1.0 **INTRODUCTION**

1.1 This Corporate Policy is intended for use by persons involved in the use of covert surveillance or a covert human intelligence source under the Regulation of Investigatory Powers Act 2000 ("the Act"). Part II of the Act deals with surveillance and covert human intelligence sources ("CHIS"). In addition, in 2018 the Secretary of State issued revised Codes of Practice on Covert Surveillance and Property Interference and Covert Human Intelligence Sources ("the Codes of Practice") pursuant to Section 71 of the Act. The Council should have regard to the Codes of Practice when exercising its powers under Part II of the Act. This Corporate Policy is based on the Codes of Practice.

1.2 Conduct to which Part II of the Act applies is lawful for all purposes if it is conduct which is authorised under the Act and the conduct is in accordance with or pursuant to the authorisation. In addition, any officer will not be subject to any civil liability in respect of any conduct of his which is incidental to any lawful conduct. It is therefore important that any officer seeking to use powers under Part II of the Act has regard to the Codes of Practice and the contents of this Corporate Policy.

1.3 This Corporate Policy, along with the Codes of Practice published by the Secretary of State, are readily available at Pendle Borough Council for consultation and reference. Copies of this Corporate Policy can be obtained from the Head of Legal Services, Town Hall, Market Street, Nelson BB9 7LG. It is also available on the Council's website.

2.0 **DEFINITIONS**

The following definitions are used in this Corporate Policy.

2.1. **Directed Surveillance**

2.1.1 Part II of the Act relates to directed surveillance. Surveillance is directed surveillance if all the following are true:-

(a) It is covert but not intrusive surveillance.

(b) It is conducted for the purposes of a specific investigation or operation.

(c) It is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

(d) It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which are such that it would not be reasonably practicable for an authorisation under Part II of the Act to be sought.

2.2.0 **Covert Surveillance**

2.2.1 Surveillance is covert only if it is carried out in a manner that is calculated to ensure that persons who are subject to it are unaware that it is or may be taking place.

2.3.0 Limitation on the use of Directed Covert Surveillance

2.3.1 Local Authorities are permitted under the Act to authorize directed covert surveillance on the ground that such surveillance is necessary for the prevention or detection of crime. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment)

Order 2012 restricts Authorising Officers in a local authority in England or Wales from authorising the carrying out of directed surveillance unless it is for the purpose of preventing or detecting a criminal offence which meets the following conditions:

- That the criminal offence to be prevented or detected is punishable by a maximum terms of at least six months' imprisonment, or

- The criminal offence to be prevented or detected is an offence under Sections 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or Section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

2.3.2 It is therefore essential that applicants for authorisations consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance.

2.4.0 **Intrusive Surveillance**

2.4.1 Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle and that involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device. A surveillance device is any apparatus designed or adapted for use in surveillance. Whether something is intrusive surveillance depends on the location of the surveillance and not to any consideration of the nature of the information that is expected to be obtained. Local authorities are not permitted to undertake intrusive surveillance.

2.5.0 **Private Information**

2.5.1 Private information is any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. It includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. It also includes information about any person, not just the subject of an investigation. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy, even though acting in public and where a record is being made by the Council of that person's activities for future consideration or analysis. Private information may include personal data such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

2.6.0 **Collateral Intrusion**

2.6.1 Collateral intrusion is where there is any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation for which surveillance authorisation is being sought. It is important that consideration is given to collateral intrusion when seeking an authorisation and appropriate measures should be taken to minimise the likelihood of collateral intrusion.

2.7.0 **Confidential Information**

2.7.1 Confidential information is defined in the Codes of Practice and consists of the following categories:

- communications subject to legal privilege;
- communications between a Member of Parliament and another person on constituency matters;

- confidential personal information;
- confidential journalistic material.

Further advice on confidential information is contained at paragraph 4.5.

2.8.0 **Residential Premises**

2.8.1 Residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. However, common areas (such as a communal area in a block of flats) to which a person has access in connection with their use or occupation of the accommodation are specifically excluded from the definition of residential premises. "Premises" includes any place whatsoever, including any vehicle or movable structure whether or not occupied as land.

2.9.0 **Covert Human Intelligence Source (CHIS)**

2.9.1 A person is a CHIS if

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

2.9.2 A relationship is established or maintained for a covert purpose only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. A relationship is used covertly and information obtained is disclosed covertly only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

Human source activity falling outside CHIS definition

2.9.3 Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of a covert relationship. Further detail on each of these circumstances is provided below.

Public volunteers

2.9.4 In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that they have observed or acquired other than through a relationship, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation under the 2000 Act is required.

Example 1: A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.

Example 2: A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal

or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.

Professional or statutory duty

2.9.5 Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 are required to report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office. 2.20 Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

2.9.6 Furthermore, this reporting is undertaken 'in accordance with the law' and therefore any interference with an individual's privacy (Article 8 rights) will be in accordance with Article 8(2) ECHR.

2.9.7 This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on. For example, a travel agent who is asked by the police to find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances, a CHIS authorisation may be appropriate.

Tasking not involving relationships

2.9.8 Tasking a person to obtain information covertly may result in authorisation under Part II of the 2000 Act being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

Example: A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

Identifying when a human source becomes a CHIS

2.9.9 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

2.9.10 Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

Example: Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague.

2.9.11 However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible, therefore, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of thatmaterial for its own investigative purposes.

Special considerations for authorisations

Vulnerable individuals

2.9.12 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an individual may be vulnerable, they should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases, Annex A lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a CHIS.

Juvenile sources

2.9.13 Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

2.9.14 Public authorities must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent or guardian of the CHIS, unless they are unavailable or there are specific reasons for excluding them, such as their involvement in the matters being reported upon, or where the CHIS provides a clear reason for their unsuitability. In these circumstances another suitably qualified person should act as appropriate adult, e.g. someone who has personal links to the CHIS or who has professional qualifications that enable them to carry out the role (such as a social worker). Any deployment of a juvenile CHIS should be subject to the enhanced risk assessment process set out in the statutory instrument, and the rationale recorded in writing.

2.10.0 **Authorising Officer**

2.10.1 An authorising officer is a person within the Council who is entitled to grant authorisations under the Act. The relevant legislation provides that an authorising officer must be a person who is a Director, Head of Service, Service Manager or equivalent. The following are Authorising Officers for the Council:

Corporate Director

Head of Legal Services

2.11.0 **Senior Responsible Officer**

2.11.1 The Senior Responsible Officer is responsible for the integrity of the Council's procedures to authorise directed surveillance or the use of a CHIS. He is also responsible for ensuring compliance with the Act and the Codes of Practice and engagement with the Commissioners and Inspectors when they conduct their inspections and where necessary overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner. The Council's Senior Responsible Officer is the Head of Legal Services.

2.12.0 **RIPA Monitoring Officer**

2.12.1 This is an internal role performed by the Head of Legal Services. This role involves maintaining policies and procedures, providing training and keeping a central record of all applications and liaising with the Investigatory Powers Commissioner's Office (IPCO)..

2.13.0 **Investigatory Powers Commissioner's Office (IPCO)**

2.13.1 IPCO is the statutory body responsible for inspection and regulation of the public authorities which make use of the powers under Part II of the Act. The Council is inspected by IPCO on a regular basis and is required to provide annual statistics to IPCO of the Council's use of the powers under the Act.

3.0 **Human Rights Considerations**

3.1 Under Article 8 of the European Convention on Human Rights contained in Schedule 1 of the Human Rights Act 1998, the Council must respect an individual's right to respect for his private and family life, his home and his correspondence. However, this right is not absolute, and is qualified thus: -

"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

3.2 Any such interference must be lawful, necessary and appropriate. The Act is one of the means by which such interference can be undertaken lawfully.

3.3 Covert surveillance or the use of a CHIS can be only be undertaken if it is necessary for one of the purposes set out in the Act. In relation to local authorities the only purpose for which covert surveillance or the use of a CHIS can be undertaken is for the purpose of preventing or detecting crime or of preventing disorder.

3.4 The officer authorising the covert surveillance or use of a CHIS must believe that the authorisation is necessary and that the conduct is proportionate to what is sought to be achieved by undertaking the authorised activity.

3.5.0 **Necessity**

3.5.1 The covert surveillance/use of a CHIS must be necessary for the purpose of preventing or detecting crime or preventing disorder. Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any criminal proceedings and the apprehension of the person or persons by whom any crime was committed.

3.6.0 **Proportionality**

3.6.1 The authorising officer must believe that the conduct required by the authorisation is proportionate to what is sought to be achieved by undertaking the surveillance or use of a CHIS. This involves balancing the extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken by the Council in the public interest. Covert surveillance/use of a CHIS should be the most appropriate method of advancing the investigation. Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. Efforts should be made to minimise the amount of collateral intrusion (see paragraph 4.4 for further details). The applicant should draw attention to any circumstances that give rise to a meaningful degree of collateral intrusion.

3.6.2 An interference with the right to respect of individual privacy may not be justified because the adverse impact on the privacy of an individual or group of individuals is too severe. Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation or is in any way arbitrary will not be proportionate and should therefore be refused.

3.7 **Social Media**

3.7.1 It should not be assumed that all monitoring of open social media sites are automatically immune from the need for an authorisation of some sort. Use of open media, in circumstances where there is a reasonable expectation of privacy, is likely to require an authorisation, particularly if the monitoring is intensive or for a prolonged period of time i.e. more than a week or so. The creation of fake or anonymous websites for investigation purposes is likely to require an authorisation. Entry on to chat rooms or closed groups for investigatory purposes is also likely to require authorisation unless the officers identity is made clear from the outset. Use of a 3rd party's identity requires both an authorisation and express written permission from that person. Whilst overt working in this way might avert the need for a surveillance authorisation officers should be aware that a CHIS situation could inadvertently arise.

3.7.2 It is expected that social media sites will generate significant amounts of sensitive information. Sensitive material that is not relevant to an investigation should be quickly and safely disposed of. Any interaction between an investigator and the public via social media could inadvertently give rise to a CHIS situation. Investigators should generally avoid interaction whilst monitoring social media

sites and take advice should any uncertainty arise. The use of internet and social media may require a RIPA Authorisation in the following circumstances:

1. Any Communications which are made with 3rd parties for the purpose of gathering evidence or intelligence about an offence in circumstances where the third party is not aware that the officer is working for the Local Authority.
2. Accessing private pages of social media for the purpose of gathering evidence or intelligence about an offence or other matter subject to potential litigation
3. Communication between an officer and a 3rd party for the purpose of using that person to gather evidence or intelligence about a suspect.
4. Intensive monitoring of a suspect using social media over a sustained period of time particularly when this is used in connection with other methods of investigation.
5. Creation of a false persona or use of a third parties identity for investigation purposes
6. Any direct interaction in any forum – open or closed – in which an officer seeks to elicit information, if they are not explicit about their real identity.

Repeated entry to social media sites and copying material for the purpose of an investigation is likely to engage the RIPA regime. As a rule of thumb access to Facebook and other social media sites should be made via the Council's Facebook account as opposed to a private account. If there is any doubt the officer who is conducting this activity is advised to take legal advice.

The Council has a seperate Social Media Policy

4.0 The Authorisation Process

4.1 Authorisation

4.1.1 An authorisation must be given by an authorising officer in writing.

4.1.2 Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable.

4.2.0 Completion of Application Form

4.2.1 The applicant should complete an application form (available on the Council's intranet) either in writing or electronically, setting out for consideration of the authorising officer the necessity and proportionality of a specific application. The application completed by the applicant must also include:

- the reasons why the authorisation is necessary in the particular case for the purpose of preventing or detecting crime or of preventing disorder;
- the nature of the surveillance;
- the identities (where known) of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where appropriate;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;

- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the level of authority required for the surveillance; and
- a subsequent record of whether the authorisation was given or refused, by whom and the time and date this happened.

4.3 **Necessity, Proportionality and Collateral Intrusion Considerations**

4.3.1 Applicants must consider the issues of necessity, proportionality and collateral intrusion on the application form.

4.3.2 Necessity should be a short explanation of the crime or disorder which is the subject of the proposed surveillance and why it is necessary to use surveillance or a CHIS.

4.3.3 In the proportionality section of the application form, applicants should outline what they expect to achieve from the surveillance and explain how the level of intrusion is justified when taking into consideration the benefit the information will give to the investigation. The applicant must believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not of itself render intrusive actions proportionate. It will not be appropriate to use covert techniques for minor offences such as dog fouling. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

4.3.4 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing as far as reasonably practicable what other methods have been considered and why they were not implemented.

4.3.5 Collateral intrusion should also be addressed. Measures should be taken wherever practicable to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subject of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised provided the intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

4.3.6 Notes to assist applicants and authorising officers in completing forms are contained at Appendices 1 and 2. Further guidance on the completion of application forms and necessity and proportionality considerations is contained in the Codes of Practice.

4.4 **Confidential Information**

4.4.1 The Codes of Practice require particular care to be taken in cases where the subject of the investigation or operation is likely to result in the obtaining of confidential information. Any application where confidential information is likely to be obtained can only be authorised by the Chief Executive. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection. The following categories of information are regarded as confidential information.

4.4.2 **Matters Subject to Legal Privilege**

This means information such as confidential written/oral communications between a professional legal adviser and his client or any person representing his client in connection with the giving of legal advice to the client and in connection with or contemplation of and for the purpose of legal proceedings. An application for surveillance likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. Further guidance on authorisations in respect of legally privileged information is contained in the Codes of Practice.

4.4.3 **Communications between a Member of Parliament and Another Person on Constituency Matters**

This means information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. A Member of Parliament includes Members of both Houses of Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.4.4 **Confidential Personal Information**

This means information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Spiritual counselling means conversations between a person and a religious authority acting in an official capacity, where the individual being counselled is seeking or the religious authority is imparting forgiveness, absolution or the resolution of conscience in accordance with their faith. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.4.5 **Confidential Journalistic Material**

This includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4.5 **Obtaining Approval from the Magistrates' Court**

4.5.1 Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to approval by the Magistrates' Court. The Protection of Freedoms Act 2012 amends the Act to require that where an Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of covert human intelligence sources, approval from the Magistrates' Court will be required. The Council will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if at the date of the grant of the authorisation or renewal of an existing authorization they are satisfied that:

(a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a covert human intelligence source was reasonable and proportionate and that these grounds still remain.

(b) the "relevant conditions" were satisfied in relation to the authorization. These relevant conditions include the following:

(i) the relevant person was duly designated as an Authorising Officer;

(ii) it was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with.

(iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under Section 25(3) of the Act.

(iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash the authorisation.

4.5.2 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates' Court to that authorisation has been obtained.

4.5.3 To ensure compliance with this requirement, any Authorising Officer who proposes to approve an application for the use of directed surveillance or for the use of a covert human intelligence source must immediately inform the Democratic and Legal Manager by e mail of the details of the authorisation. The Democratic and Legal Manager will then make the necessary arrangements for an application for an order to approve the authorisation to the Magistrates' Court. The Authorising Officer and the applicant may be required to attend the Magistrates' Court to support the application.

5.0 **Reviews of Authorisations**

5.1 Authorisations for directed surveillance last for three months from the date on which they are granted by the authorising officer. Authorisations should be subject to a monthly review to assess the need for the surveillance to continue. The review date should be noted on the application form by the authorising officer. Reviews should normally be carried out by the authorising officer who granted the authorisation but if he or she is unavailable, the review can be conducted by another authorising officer.

5.2 Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in further or greater intrusion into the private life of any person should be brought to the attention of the authorising officer by means of a review. The authorising officer should then consider whether the proposed changes are proportionate (bearing in mind any extra intrusion into privacy or collateral intrusion) before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed. During a review, the authorising officer may amend specific aspects of the authorisation e.g. to cease surveillance of a particular suspect.

6.0 **Renewal of Authorisations**

6.1 As mentioned in paragraph 5, authorisations last for three months. However, before they cease to have effect, authorisations can be renewed for a further period of three months, using the renewal form available on the intranet. The Head of Legal Services will then make the necessary arrangements for an application for an order to approve the renewal of the authorisation to the Magistrates' Court. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Authorisations should be renewed by the officer who

granted the original authorisation but in his or her absence any authorising officer may authorise a renewal. The authorising officer for the renewal must consider it necessary for the authorisation to continue for the purpose for which it was given. The renewals last for three months and take effect on the day the existing authorisation would have expired. Authorisations can be renewed more than once provided they continue to meet the criteria for authorisation.

6.2 All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously
- any significant changes to the information in the initial application
- the reasons why the authorisation for directed surveillance should continue
- the content and value to the investigation or operation of the information so far obtained by the surveillance
- the results of regular reviews of the investigation or operation

7.0 Cancellation of Authorisations

7.1 An authorisation must be cancelled by an authorising officer if he is satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. The original applicantmust complete a cancellation form which is available on the intranet. If the original applicant is no longer available, the cancellation can be performed by an authorising officer. As soon as the decision is taken that the directed surveillance should be discontinued, the instruction must be given to all those involved to stop all surveillance of the subject.

8.0 Surveillance of Council Employees

8.1 Following the decision of the Investigatory Powers Tribunal in the case of *C v The Police and the Secretary of State for the Home Office – IPT/03/32/H* dated 14 November 2006, Councils may only engage the Act when in performance of their "core functions". These are the specific public functions undertaken by local authorities e.g. dealing with the prevention and detection of crime, such as housing and council tax benefit fraud, in contrast to the ordinary functions which are undertaken by all authorities e.g. employment issues, contractual arrangements, etc. The disciplining of an employee is not a core function, although related criminal investigations may be. The protection of the Act may therefore be available in relation to associated criminal investigations so long as the activity is deemed to be necessary and proportionate.

8.2 Surveillance which falls outside the Act should be dealt with in accordance with the Data Protection Act and the Employment Practices Code issued by the Information Commissioner's Office. For further guidance on this matter you should refer to the Council's Legal Section.

9.0 Maintenance of Records

9.1 The RIPA Monitoring Officer maintains a central record of applications. The original of all application, review, renewal and cancellation forms should be forwarded to the RIPA Monitoring Officer for inclusion on the central record. The forms should be sent in sealed envelopes to protect confidentiality. A unique reference number is allocated to each authorisation granted and is used to reference the operation/investigation throughout the duration of the activity. All these records are made available for inspection by IPCO.

9.2 Copies of all forms should be kept for a period of three years after the conclusion of any court proceedings the authorisations related to or until the next visit by IPCO, whichever is the later. This is to ensure compliance with the GDPR and Data Protection Act 2018 as respects data retention restrictions.

10.0 **Authorisation of a CHIS**

10.1 There must be arrangements in place for ensuring that at all times a designated Council Officer has responsibility for maintaining a record of the use made of the CHIS and that records that disclose the identity of the CHIS will only be disclosed to persons who have a need for access to them.

10.2 Arrangements must also be in place for ensuring that at all times a designated Council officer has day to day responsibility for dealing with the CHIS on behalf of the Council and the CHIS's security and welfare. This officer will be known as a handler and will usually be of a rank or position below that of the authorising officer. The handler will have day to day responsibility for:

- dealing with the CHIS on behalf of the Council
- directing the day to day activities of the CHIS
- recording the information supplied by the CHIS
- monitoring the CHIS's security and welfare

10.3 At all times another designated Council officer must have general oversight of the use made of the CHIS. This officer will be known as the controller and will normally be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

10.4 The authorisation of a CHIS lasts for 12 months but should be subject to monthly review by an authorising officer.

10.5 Pendle Borough Council Council does not generally use a CHIS and any request to do so should be referred to the RIPA Monitoring Officer in the first instance for guidance and advice. Further guidance is contained in the relevant Code of Practice.

NOTES FOR APPLICANTS

Officers seeking an authorisation to undertake directed surveillance should:

1. Familiarise themselves with the Act and read the Council's Corporate Policy and the Home Office Code of Practice on Covert Surveillance and Property Interference. The Council's Corporate Policy and the Home Office Code of Practice can be accessed via the Council's intranet site by entering 'RIPA' into the search facility.

2. Obtain the appropriate forms from the Council's intranet site on each and every occasion. Do not alter the forms**.** There are separate forms for directed surveillance and covert human intelligence sources.

3. Obtain a unique reference number for use on applications etc relating to a particular investigation from the RIPA Monitoring Officer.

4. Complete, sign and date the relevant form (application, review, renewal or cancellation) and submit to an authorising officer for authorisation. Details of the Council's authorising officers are available on the Council's intranet site.

5. When the applicant receives an authorisation, he should keep a copy and ensure the original signed authorisation is sent to the Council's RIPA Monitoring Officer.

6. Authorisations run from the date and time they are given and not from the commencement of the surveillance.

7. Authorisations always last for 3 months e.g. an authorisation granted on 29th April expires on 28th July. If the applicant only expects to undertake surveillance over a few days or weeks, he should ensure that a cancellation form is completed as soon as the surveillance has ended, rather than waiting until the end of the 3 month authorisation period to expire.

8. Ensure that review forms are completed and authorised by an authorising officer every month while the authorisation remains in force.

9. If authorisation of the surveillance is needed beyond the expiry date given on the form (which will be 3 months from the date of authorisation), the applicant should be aware of the authorising officer's need to complete a renewal form and put this into place before the end of the authorised period.

10. A renewal form should not be completed by the applicant until shortly before the existing authorisation period is due to expire. A copy of the signed renewal form should be retained by the applicant and the original signed form should be sent to the Council's RIPA Monitoring Officer.

11. If the surveillance is no longer needed the applicant should immediately complete a cancellation form which should be signed by an authorising officer. A copy of this form should be retained by the applicant and the original signed form should be sent to the Council's RIPA Monitoring Officer.

12. If the surveillance has been carried out in accordance with a written authorisation, i.e. if the paperwork is in order, the surveillance is lawful for all purposes.

NOTES FOR AUTHORISING OFFICERS

Authorising Officers should:

1. Familiarise themselves with the Act and read the Council's Corporate Policy and the Home Office Code of Practice on Covert Surveillance and Property Interference. The Council's Corporate Policy and the Home Office Code of Practice can be accessed via the Council's intranet site by entering 'RIPA' into the search facility.

2. Read and carefully assess all applications for the use of surveillance (and renewals if the surveillance is expected to go on for longer than the statutory 3 months).

3. Ensure that a unique reference number given by the RIPA Monitoring Officer appears in the box at the top of the form.

4. Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially where it is necessary to act urgently. Where an authorising officer authorises such an investigation or operation, the central record of authorisations should record this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

5. Authorising officers should grant an authorisation only if it is necessary for the purpose of preventing or detecting crime or of preventing disorder and it is proportionate, bearing in mind the risks of collateral intrusion and the obtaining of confidential material.

6. When completing an authorisation, authorising officers must ensure that they put onto the authorisation where indicated, details of the activity they are granting to ensure the parameters of the activity being authorised are accurately defined by them as authorising officers**.**

7. Authorising officers must enter monthly review dates on any application or renewal form they are asked to authorise.

8. All application, review, renewal or cancellation forms should be signed, dated and timed by the authorising officer e.g. 29th April 2010 at 15.00.

9. Authorisations run from the date and time they are given and not from the commencement of the surveillance.

10. Authorisations always last for 3 months. Authorising officers must enter a cancellation date and time (which should be 23.59) on the application form e.g. an authorisation granted on 29th April expires on 28th July at 23.59.

11. Authorising officers should keep a note in their diary of the date upon which the authorisation was granted and a date no later than one month ahead for a review to be carried out.

12. Authorising officers must complete a review form a month after the granting of authorisation or (if required) complete the form to comply with an earlier review date of his /her own choosing. Some Service Units may wish to review authorisations after one or two weeks depending on the expected length of the particular investigation. However reviews should not be left for longer than a month.

13. Review, renewal and cancellation forms should be authorised by the authorising officer who granted the original authorisation. If for whatever reason the original authorising officer is not available, any authorising officer can sign the review, renewal or cancellation form.

14. A renewal form must be completed if the surveillance is to continue beyond the date given on the application form for the surveillance to end. Authorising officers should check the original

application form if they are unsure. A renewal form must be completed before the expiry date on the application form so as to leave no gaps. If a gap is found to have been left between expiry of the authorisation and renewal, a renewal form cannot be used and a new application form must be completed immediately. Note that any surveillance activity carried out during the gap between authorisations is not covered under the Act. Officers should be prepared for an argument in court about a breach of Article 8 of the European Convention on Human Rights should they decide they must still use the evidence.

15. A renewal form should not be authorised until shortly before the existing authorisation period is due to expire. The renewal form should be dated and timed by the authorising officer from midnight on the day the previous authorisation expires e.g. 00.00 on 28th July.

16. A cancellation form must be completed as soon as the surveillance is no longer necessary or proportionate, and at any rate before the expiry of the authorisation, which could be anytime before the expiry of 3 months from the date of authorisation. Authorising officers should check the expiry date given on the form. The applicant will normally ask for the cancellation but if he does not and the authorising officer thinks it should be cancelled he/she must do so immediately. The date and time of the cancellation must be recorded on the form by the authorising officer.

17. Authorising officers should send the original signed application, review, renewal or cancellation forms to the RIPA Monitoring Officer in a sealed envelope and provide the applicant with a copy

18. If the RIPA Monitoring Officer issues a corrective action form highlighting issues on an application, review, renewal or cancellation form, it is the responsibility of the authorising officer to communicate these to the applicant, or consider his or her own part in the issues, and put in place measures to ensure that these are not repeated. The corrective action form should be returned to the Monitoring Officer with appropriate action/comments recorded by the authorising officer.

19. Authorising officers should be aware that their action in completing these forms could come under judicial scrutiny in the event of a dispute and that they may find themselves giving evidence in Court and/or being cross-examined about one of their authorisations or the Council's systems and procedures.

20. Authorising officers responsible for the granting of higher level authorisations must complete refresher training.

21. If you cease to be an authorising officer, then the RIPA Monitoring Officer should be informed. Each new appointment of an authorising officer needs to be communicated to the RIPA Monitoring Officer.

APPENDIX 3

LIST OF AUTHORISING OFFICERS

Corporate Director

Head of Legal Services