

WEST LANCASHIRE BOROUGH COUNCIL

RIPA POLICY

The Regulation of Investigatory Powers Act 2000

In respect of

Directed Surveillance, Use of Covert Human Intelligence Sources and Accessing Communications Data

Version : No.10 - 2021

RIPAPOLICYVERSION10-2021

Contents		Page
1.	INTRODUCTION	3 – 4
2	DIRECTED SURVEILLANCE	4 – 6
3.	COVERT USE OF HUMAN INTELLIGENCE SOURCE (CHIS)	7
4.	COMMUNICATIONS DATA	8
5.	AUTHORISATIONS, RENEWALS AND DURATION	8 – 14
6.	REVIEWS	15
7.	RENEWALS	15
8.	CANCELLATIONS	16
9.	CENTRAL REGISTER OF AUTHORISATIONS	16 – 17
10.	CODES OF PRACTICE	17
11.	BENEFITS OF OBTAINING AUTHORISATION UNDER THE 2000 ACT	17 – 18
12.	SCRUTINY AND TRIBUNAL	18
	APPENDICES	
	APPENDIX 1 - DEFINITIONS FROM THE 2000 ACT	20 – 21
	APPENDIX 2 - NOTIFICATION TO CENTRAL REGISTER OF AUTHORISATIONS UNDER RIPA	22
	APPENDIX 3 – CHART SETTING OUT THE RIPA MANAGEMENT STRUCTURE	23
	APPENDIX 4 – THE OFFICE OF INVESTIGATORY POWERS COMMISSIONER’S GUIDANCE – COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES	25

1 INTRODUCTION

- 1.1. The Regulation of Investigatory Powers Act 2000 (the 2000 Act) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected consistent with the obligations under The Human Rights Act 1998, while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.
- 1.2. West Lancashire Borough Council is therefore included within the 2000 Act framework with regard to the authorisation of Directed Surveillance, the use of Covert Human Intelligence Sources (CHIS) and the obtaining of communications data through a single point of contact (SPOC).
- 1.3 The purpose of this guidance is to:
 - explain the scope of the 2000 Act and the circumstances where it applies
 - provide guidance on the authorisation procedures to be followed.

This continues to be a developing area of law and the Courts are yet to fully define the limits of the powers. This should be borne in mind when considering this Guide.

- 1.4 The Council has had regard to the Codes of Practice on covert surveillance, CHIS and accessing communications data produced by the Home Office in preparing this guidance and each Service should hold copies to which staff can refer. These documents are available at www.homeoffice.gov.uk/ripa.
- 1.5 In summary the 2000 Act requires that when the Council undertakes “directed surveillance”, uses a “covert human intelligence source or accesses communications data (defined below at paragraphs 2, 3 and 4 below) these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied.
- 1.6 The Chief Operating Officer, Corporate Director of Place and Community and, Corporate Director of Transformation and Resources can authorise these activities (in relation to communications data, they shall be known as Designated Persons and shall seek the advice of the SPOC, see further paragraphs 4 and 5.1.3 below). Such nomination permits officers to grant authority for any purpose under the terms of the 2000 Act across all Council Services and service areas.
- 1.7 **Once an authorisation is granted for the use (or renewal) of directed surveillance, or acquisition of communications data, or covert human intelligence source it cannot take effect without an order approving the grant (or renewal) being obtained from a single Justice of the Peace (Magistrate, District Judge) (under amendments made by the Protection of Freedoms Act 2012, to s.32A and s.32B of the 2000 Act). This order must be sought from the Magistrates’ Court, but when the Court is not in session. The arrangements for seeking the order will be made in consultation with Legal Services.**
- 1.8 Authorisation under the 2000 Act gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation helps to protect the Council and

its officers from complaints of interference with the rights protected by Article 8(1) of the European Convention on Human Rights, i.e. the right to respect for private and family life which is now enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be “in accordance with the law”. Provided activities undertaken are also “reasonable and proportionate” they will not be in contravention of Human Rights legislation.

- 1.9 Authorising Officers and investigators within the Local Authority are to note that the 2000 Act does not extend to powers to conduct intrusive surveillance. Investigators should familiarise themselves with the provisions of Sections 3, 4 and 5 of the Code of Practice on Directed Surveillance to ensure a good understanding of the limitation of powers within the 2000 Act.
- 1.10. Deciding when authorisation is required involves making a judgment **and assessing whether specific conditions apply to the investigation target**. Paragraph 3.4 explains this process in detail. If you are in any doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Legal and Democratic Services Manager/Senior Responsible Officer. However, in those cases where there is doubt as to the need for an authorisation it may be safer to consider seeking/granting an authorisation: a broader reading of the application of the Act’s requirements is encouraged.
- 1.11. In the case of CHIS authorisations for vulnerable people or juveniles, or where surveillance involves communication subject to legal privilege, confidential personal information or confidential journalistic material authorisation must be obtained from the Chief Operating Officer only, **together with the necessary application for an order giving effect to authorisation from a Justice of the Peace**.
- 1.12 The Chief Operating Officer should be requested to authorise directed surveillance involving the covert filming of any Council member or employee to the extent that this falls within RIPA.

2. DIRECTED SURVEILLANCE

2.1 **The Council must apply to a Justice of the Peace for an order that gives effect to the authorisation for the use of directed surveillance prior to undertaking the activity.**

2.2 What is meant by Surveillance?

"Surveillance" includes:

- a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
- b) recording anything monitored, observed or listened to in the course of surveillance; and
- c) surveillance by or with the assistance of a surveillance device.

2.3 When is surveillance directed?

Surveillance is 'Directed' for the purposes of the 2000 Act if it is covert, but not intrusive and is undertaken:

- a) for the purposes of a specific investigation or a specific operation.
- b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
- c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

2.4 In certain circumstances, use of social media sites such as Facebook, or using the internet in other ways could need authorisation as directed surveillance. The Office of Surveillance Commissioners has given guidance on when the use of social media and the internet might need authorisation on RIPA. The guidance can be read at appendix 4.

2.5 Surveillance Threshold

2.5.1 Before directed surveillance can be undertaken and the requisite order from a Justice of the Peace applied for, the Council must be satisfied that they are investigating a criminal offence that carries a maximum sentence of 6 months or more imprisonment.

2.5.2 The exception to the 6 month sentence threshold is specific offences of sale of alcohol or tobacco to an underage person which does not fall within the Council's range of regulatory activities.

2.5.3 During the course of an investigation, should the Council become aware that the criminal activity under investigation falls below the 6 month sentence threshold, then use of directed surveillance should cease.

2.5.4 This 6 month sentence threshold does not apply to use of covert human intelligence or communications data techniques.

2.6 The Council cannot undertake intrusive surveillance.

2.6.1 Surveillance becomes intrusive if the covert surveillance:

- a) is carried out in relation to anything taking place on any "residential premises" or in any "private vehicle"; and
- b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or
- c) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of

the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

2.7 Before any officer of the Council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within the 2000 Act. In order to do this the following key questions need to be asked.

2.7.1 Is the surveillance covert?

Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place.

If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not in general apply. However, if there is any doubt in respect of this matter, an officer must consider whether it may be appropriate to seek a RIPA authorisation.

2.7.2 Is it for the purposes of a specific investigation or a specific operation?

For example, are Civic building CCTV cameras which are readily visible to anyone walking around the building covered?

The answer is not if their usage is to monitor the general activities of what is happening in the car park. If that usage, however, changes, the 2000 Act may apply.

For example, if the CCTV cameras are targeting a particular known individual, and are being used in monitoring his activities, that has turned into a specific operation which may require authorisation.

2.7.3 Is it in such a manner that is **likely** to result in the obtaining of private information about a person?

"Private information" is any information relating to a person's private or family life and aspects of business or professional life.

For example, if part of an investigation is to observe a member of staff's home to determine their comings and goings then that would be covered.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework. However, the use of 'test purchasers' may involve the use of covert human intelligence sources (see later).

If in doubt, it is safer to consider getting authorisation.

2.7.4 Is it undertaken **otherwise than by way of an immediate response to event or circumstances where it is not reasonably practicable to get authorisation?**

The Home Office gives the example of an immediate response to something happening during the course of an observer's work, which is unforeseeable.

However, if as a result of an immediate response, a specific investigation subsequently takes place that brings it within the 2000 Act framework.

2.7.5 Is the Surveillance Intrusive?

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

Commercial premises and vehicles are therefore excluded from intrusive surveillance. **The Council is not authorised to carry out intrusive surveillance.**

2.7.6 Does the offence under investigation meet the 6 month threshold?

3 COVERT USE OF HUMAN INTELLIGENCE SOURCE (CHIS)

3.1 A person is a Covert Human Intelligence Source 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 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.

3.2. A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

3.3. The above clearly covers the use of professional witnesses to obtain information and evidence. It is not Council practice to use such witnesses. It can also cover cases such as a Council officer making a test purchase when there is a need to cultivate a relationship with the seller, which would not usually be the case.

3.4. There is a risk that an informant may be, or become, a CHIS. A member of the public giving information will be a CHIS if the information which he covertly passes to the authority has been obtained in the course of (*or as a consequence of the existence of*) a personal or other relationship. See paragraph 2.24 of the CHIS Code of Practice. Also consider paragraph 270 of OSC Procedures and Guidance 2011, which refers to the risk of "status drift". When an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship, alarm bells should begin to ring. It probably means that the informant is in reality a CHIS, to whom a duty of care is owed if the information is then used. In such circumstances officers should refer any such instance for legal advice before acting on the information received from such an informant.

3.5 In this context (of authorising CHIS) ANY information (ie not confined to private information alone) to be gained by the covert manipulation of a relationship will

require authorisation.

3.6 The Council must apply to a Justice of the Peace for an order that gives effect to the authorisation for the use of covert human intelligence source (see 1.7 above).

3.7 In certain circumstances, use of social media sites such as Facebook, or using the Internet for research in other ways could need authorisation as the use of a covert human intelligence source. The guidance can be read at appendix 4.

4 COMMUNICATIONS DATA

4.1 The Council may also access certain communications data under the 2000 Act, provided this, like all other surveillance, is **for the purpose of preventing or detecting crime**.

4.2 Following the passage of the Data Retention and Investigatory Powers Act 2014 the Home Office has revoked all accreditation which enabled local authority staff to acquire communications data with effect from 1 December 2014. The Council is now required to use the National Anti-Fraud Network's (NAFN's) Single Point of Contact (SPOC) services to acquire communications data under RIPA, if approved by a magistrate. The Acquisition and Disclosure of Communications Data Code of Practice shall be followed at all times. Council staff are not permitted to obtain telecommunications and internet use data other than as provided for by the Act.

4.3 The Council must apply to a Justice of the Peace for an order giving effect to the authorisation of the use of communications data.

4.4 The accredited SPOCs at NAFN will scrutinise the applications independently. They will provide advice to applicants and designated persons ensuring the Council acts in an informed and lawful manner.

5. AUTHORISATIONS, RENEWALS AND DURATION

5.1 The Council must apply to a Justice of the Peace for an order that gives effect to the authorisation for the use of directed surveillance, communications data and covert human intelligence source (see 1.7 above).

5.1.1 The Conditions for Authorisation

5.1.2 Directed Surveillance

5.1.1.3 For directed surveillance no officer shall grant an authorisation **and make an application to a Justice of the Peace** for the carrying out of directed surveillance unless he believes:

- a) that an authorisation is necessary for the purpose of preventing or detecting crime and
- b) the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

- 5.1.1.4 The onus is therefore on the person authorising such surveillance to satisfy themselves it is:
- a) necessary for the ground stated above and;
 - b) proportionate to its aim.

5.1.1.5 In order to ensure that authorising officers have sufficient information to make an informed decision **about whether to make an application to a Justice of the Peace for an order to give effect to any authorisation**, it is important that detailed records are maintained. As such the forms in the Appendix and the accompanying Guidance on Completing RIPA Authorisation Forms are to be completed where relevant.

It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against that which has been authorised.

An Authorising Officer may partially approve or partially refuse an application for authorisation. If an Authorising Officer does not authorise all that was requested, a note should be added explaining why.

5.1.2 Covert Use of Human Intelligence Sources

5.1.2.1 The same principles as Directed Surveillance apply. (see paragraph 5.1.1.3 above)

5.1.2.2 The conduct so authorised is any conduct that:

- a) is comprised in any such activities involving the use of a covert human intelligence source, as are specified or described in the authorisation;
- b) relates to the person who is specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and
- c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

5.1.2.3 In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. As such the forms attached are to be completed where relevant.

It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against that is authorised.

5.1.3 Communications Data

Section 22(4) of RIPA allows the Council to request “communications data” from Communication System Providers (CSPs). The access allowed under these powers is limited to telephone, postal and email subscriber and billing information. Any access must be obtained through the use of an authorised single point of contact (SPOC). (See Communications Data Code of Practice paragraphs 4.4 –

4.9.) The Council does not have the right to obtain the content of the communication, but can obtain details of the source and destination of a message. The only ground for Local Authorities is the prevention or detection of crime. CSPs must be provided with a Notice Requiring Disclosure of Communications Data, which must have been duly authorised. The only officers who are allowed to authorise such requests are those accredited by the Home Office (the “Designated Persons” (DPs)). The DP is an individual at the level of Chief Operating Officer and Corporate Director and will scrutinise all applications for Communications Data.

The authorisation or grant of a notice to obtain communications data require judicial approval on each occasion.

5.2 Further Requirements of the 2000 Act

5.2.1 An application must be made to the Justice of the Peace for an order that gives effect to the authorisation for the use of Directed Surveillance, Communications Data and CHIS. This process is in addition to the Council’s existing authorisation procedure (see 1.7 above).

5.2.2 In light of the changes to the regime applications for urgent grants or renewal, must be in writing. In the Guidance on Completing RIPA Authorisation Forms document which accompanies this Guide are standard forms, which must be used. Officers must direct their mind to the circumstances of the individual case with which they are dealing when completing the form.

5.2.3 Although it is possible to combine two authorisations in one form the Council’s practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a CHIS.

5.2.4 Authorisations lapse, if not renewed:

- 12 months - if in writing/non-urgent - from date of last renewal if it is for the conduct or use of a covert human intelligence source or
- in all other cases (ie directed surveillance) 3 months from the date of their grant or latest renewal.

5.2.5 Any person entitled to grant a new authorisation can renew subject to judicial approval being obtained an existing authorisation in the same terms at any time before it ceases to have effect.

But, for the conduct of a covert human intelligence source, an Authorised Officer should not renew **or make an application to a Justice of the Peace to renew** unless a review has been carried out and that person has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

5.2.6 The benefits of obtaining an authorisation are described in paragraph 7 below.

5.2.7 Factors to Consider (see further guidance the Guidance on Completing Forms

document)

Any person giving an authorisation should first satisfy him/herself that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve. The proportionate test involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

5.2.8 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

5.2.9 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. The authorising officer will take this into account, particularly when considering the proportionality of the surveillance and whether measures to avoid can be stipulated.

5.2.10 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

5.2.11 Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

Home Surveillance

5.2.12 The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance at his/her home (NB. the Council cannot undertake intrusive surveillance) or where there are special sensitivities.

Spiritual Counselling

5.2.13 No operations should be undertaken in circumstances where investigators believe that surveillance will lead them to intrude on spiritual counselling between a Minister and a member of his/her faith. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.

Confidential Material

5.2.14 The 2000 Act allows in exceptional circumstances for authorisations to gather 'confidential material' (see the definitions in Appendix 1). Such material is particularly sensitive, and is subject to additional safeguards under this code. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to special authorisation (by the Chief Operating Officer).

5.2.15 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

5.2.16 The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Legal and Democratic Services Manager/Senior Responsible Officer before further dissemination takes place;
- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Legal and Democratic Services Manager/Senior Responsible Officer) is satisfied that it is necessary for a specific purpose;
- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information;
- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose;
- Any covert surveillance concerning premises on which legal consultations take place are to be regarded as intrusive surveillance and may not be undertaken by the Council.

Combined authorisations

5.2.17 Although it is possible to combine two authorisations in one form the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a CHIS.

5.2.18 In cases of joint working with other agencies on the same operation, e.g. by a Housing Benefit Investigator authority for directed surveillance should be given by the lead agency.

5.2.19. On occasion, several Council Services may be included in the same investigation. One authorisation from the Lead Service should cover all activities.

Handling and disclosure of product

5.2.20 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 5.2.16 above.

5.2.21 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

5.2.22 Authorising Officers must ensure that the relevant details of each authorisation are sent to the Legal and Democratic Services Manager/Senior Responsible Officer as described in paragraph 9 below.

5.2.23 The originals of applications for authorisations, reviews, renewals and cancellations for directed surveillance and the use of a CHIS should be submitted to and thereafter retained by the RIPA Co-ordinator, for a period of 3 years and at least between inspections. Copies are to be retained by the authorising officer for a commensurate period. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

5.2.24 Any personal data collected during the course of a covert surveillance operation must be stored as per data protection guidelines set out in the Council's Data Protection Policy below.

- Analysis of data from the operation must be carried out by the officers who carried out the investigation and should be done in a private office to avoid personal material being accessible to other council employees.
- The authorising officer may also be included in analysis of the data collected.
- Data must be kept in a secure environment with limited access.
- Data must be labelled with the reference of the case and the date of collection.
- Data collected which is not appropriate or useful as evidence in the investigation and subsequent formal action must be deleted as soon as this fact is determined or when the case is closed, whichever is the sooner. Consideration of whether or not this material should be destroyed is the responsibility of the senior authorising officer. Care must be taken in this respect, as it must be considered that even if this information is not to be used as evidence, it may be "unused material" for the purposes of criminal proceedings.

- If there is any reason to believe that the data obtained during the course of an investigation might be relevant to that investigation, or to another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed but retained in accordance with established disclosure requirements and may be disclosed.

5.2.25 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the Council, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

5.3 **The Use of Covert Human Intelligence Sources**

5.3.1 The Council will not normally use an external or professional source for the purpose of obtaining information. It is not the Council's usual practice to seek, cultivate or develop a relationship through an external or professional source although this may occur where circumstances require it. In these circumstances appropriate authorisations must be obtained. It is potentially possible, though highly unlikely, that the role of a Council employee may be that of a source, for example, as contemplated in paragraph 3.3 above, please cross refer for detail.

5.3.2 Nothing in the 2000 Act prevents material obtained by an employee acting as a source being used as evidence in Court proceedings.

5.3.3 The Authorising Officer must consider the safety and welfare of an employee acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration from the start for the safety and welfare of the employee, even after cancellation of the authorisation, should also be considered.

5.3.4 The Authorising Officer must believe that the authorised use of an employee as a source is proportionate to what it seeks to achieve. Accurate and proper records should be kept about the source and tasks undertaken.

5.3.5 The Council's practice is not to use an employee acting as a source to infiltrate existing criminal activity, or to be a party to the commission of criminal offences, even where this is within the limits recognised by law.

5.3.6 Before authorising the use of an employee as a source, the authorising officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

5.3.7 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation,

“confidential material” is likely to be obtained.

5.3.8 Additionally, the Authorising Officer should make an assessment of any risk to an employee acting as a source in carrying out the proposed authorisation.

6. REVIEWS

6.1. The Home Office Code of Practice for Covert Surveillance and Property Interference makes specific reference to reviews at paragraph 4.34. It recommends regular reviews be undertaken to see if the need for the surveillance is still continuing. Results of reviews should be recorded in a central record of authorisations (see paragraph 8.1). Reviews should be more frequent when access to confidential information or collateral intrusion is involved. Review frequency should be as often as the authorising officer deems necessary or practicable.

6.2. Similar provisions appear at paragraphs 8.9 – 8.11 of the code of practice for CHIS, save that tasks given to the source and information obtained should also be included.

6.3. Each authorising officer will therefore determine in each case how often authorisations should be reviewed. They will ensure records of the review will be supplied on the relevant form in Section 9 and send copies to the RIPA Co-ordinator to keep the central register up to date. Good practice requires that this should be done monthly at least.

7. RENEWALS

7.1. An authorising officer may renew an authorisation before it would cease to have effect if it is necessary for the authorisation to continue for the purpose for which it was given. **An application for a renewal to the Justice of the Peace is also required (see above).**

7.2. The Home Office Code of Practice for Covert Surveillance and Property Interference at paragraph 5.16 - 5.18 refers. A renewal of the authorisation in writing can be made for 3 months. Applications for renewal should detail how many times an authorisation has been renewed; significant changes to the original application for authority; reasons why it is necessary to renew; content and value of the information obtained so far and results of regular reviews of the investigation or operation.

7.3. Similar provisions apply in the code of practice for CHIS except that a renewal here can last for a further 12 months, a review must have been carried out on the use of the source and an application should only be made to renew when the initial authorisation period is drawing to an end. Applications to renew a CHIS also should contain use made of the source and tasks given to the source during the previous authorised period.

7.4. Each application to renew should be made at least 7 days before the authorisation is due to expire on the relevant form in Appendix 2. A record of the renewal should be kept within the applying service and supplied centrally to the Legal and Democratic Services Manager/Senior Responsible Officer - see Section 8 of the Home Office Code of Practice for Covert Surveillance and Property Interference -

to update the central register of authorisations.

8. CANCELLATIONS

- 8.1. All authorisations, including renewals should be cancelled if the need for the surveillance is no longer justified. This will occur in most cases where the purpose for which the surveillance was required has been achieved.
- 8.2. Requesting officers should ensure they inform authorising officers if this is the case before the next review. If, in the opinion of the authorising officer at the next review, the need for surveillance is no longer justified, it must be cancelled.
- 8.3. The cancellation forms at Appendix 2 will be used to record a cancellation; the original will be sent to the RIPA Co-ordinator to update the central register of authorisations and the authorising officer will retain a copy - see Section 8.
- 8.4. The Home Office Codes of Practice for both directed surveillance and CHIS make it clear that authorisations must be cancelled if the original authorising criteria are not met. With CHIS, it must be cancelled if satisfactory arrangements for the source no longer exist. Consideration for the safety and welfare of a source continues after cancellation of any authorisation.

9. CENTRAL REGISTER OF AUTHORISATIONS

- 9.1. The Codes of Practice under the 2000 Act require a central register of all authorisations to be maintained. The Senior Responsible Officer or nominated representative shall maintain this register.
- 9.2. Whenever an authorisation is granted renewed or cancelled the Authorising Officer must arrange for the following details to be forwarded by e-mail to the Senior Responsible Officer or nominated representative. Receipt of the e-mail will be acknowledged.
 - Whether it is for Directed Surveillance or CHIS ;
 - Applicants name and Job Title (manager responsible);
 - Service and Section;
 - Applicant's address and Contact Number;
 - Identity of 'Target';
 - Authorising Officer and Job Title; (in line with delegation scheme)
 - Date of Authorisation.
 - A unique reference number for the investigation or operation
 -
 - Whether confidential information is likely to be reviewed as a consequence of the investigation /operation.
 - The date the authorisation was cancelled

Details should be provided to the Senior Responsible Officer in respect of when an authorisation is refused.

See Appendix 2 for the Form of Notification

The original of the authorisation should also be provided; the authorising officer should retain a copy. The Chief Operating Officer will review authorisations every 6 months. It is suggested that authorising officers supply these directly.

- 9.3. The original authorisations shall be securely retained within the RIPA Co-ordinator's Service. It is each Service's responsibility to securely retain all copy authorisations within their Service. Authorisations should only be held for as long as it is necessary. Once the investigation is closed (bearing in mind cases may be lodged some time after the initial work) the records held by the Service should be disposed of in an appropriate manner (e.g. shredded).

10 CODES OF PRACTICE

There are Home Office codes of practice that expand on this guidance. All relevant Services hold a copy.

The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, "if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under the 2000 Act, or to one of the commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account".

Staff should refer to the Home Office Codes of Practice for supplementary guidance. These should be available to all relevant officers (see earlier).

11 BENEFITS OF OBTAINING AUTHORISATION UNDER THE 2000 ACT.

11.1 Authorisation of surveillance and human intelligence sources

The 2000 Act states that

- if authorisation confers entitlement to engage in a certain conduct and
- the conduct is in accordance with the authorisation, then
- it shall be "lawful for all purposes".

Part II of the 2000 Act does not impose a requirement on public authorities to seek or obtain an authorisation where, under the 2000 Act, one is available (see section 80 of the 2000 Act). Nevertheless, where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Public authorities are therefore strongly recommended to seek an authorisation where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

- 11.2 The 2000 Act states that a person shall not be subject to any civil liability in relation to any conduct of his which -
- a) is incidental to any conduct that is lawful by virtue authorisation; and
 - b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question

12. SCRUTINY AND TRIBUNAL

- 12.1. To effectively "police" the 2000 Act, Commissioners regulate conduct carried out thereunder. The Investigatory Powers Commissioner will keep under review, among others, the exercise and performance by the persons on whom are conferred or imposed, the powers and duties under the Act. This includes authorising directed surveillance and the use of covert human intelligence sources.
- 12.2. A tribunal has been established to consider and determine complaints made under the 2000 Act if it is the appropriate forum. Complaints can be made by persons aggrieved by conduct e.g. directed surveillance. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if:

- A Council officer has granted any authorisation under the 2000 Act.
- Council employees have engaged in any conduct as a result of such authorisation.
- A disclosure notice requirement is given.

- 12.3 The Senior Responsible Officer will ensure that a report is submitted to the Council's Audit and Governance Committee on a regular basis and that an annual report is submitted to Cabinet. The reports will include details of the overall number and type of authorisations granted and the outcome of the case, where known. In addition, the reports will provide a breakdown of the same information by service or groups of services, as appropriate. In order to comply with General Data Protection Regulation and Code of Practice requirements, no specific details of individual authorisations will be provided.
- 12.4 The RIPA Co-ordinator will maintain and check the central register of all RIPA authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the authorising officer, however, to ensure the RIPA Co-ordinator receives the original of the relevant forms as soon as possible and in any event within 1 week of authorisation, review, renewal, cancellation or rejection. The authorising officer should retain copies.

12.5 The management structure for RIPA is set out in Appendix 3.

Definitions from the 2000 Act

- **“2000 Act”** means the Regulation of Investigatory Powers Act 2000.
- **“Confidential Material”** consists of:
 - a) matters subject to legal privilege;
 - b) confidential personal information; or
 - c) confidential journalistic material.
- **Matters subject to legal privilege”** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below)
- **“Confidential Personal Information”** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:
 - a) to his/her physical or mental health; or
 - b) to spiritual counselling or other assistance given or to be given, andwhich a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office (see Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:
 - c) it is held subject to an express or implied undertaking to hold it in confidence; or
 - d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.
- **“Confidential Journalistic Material”** 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.
- **“Covert Surveillance”** means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.
- **“Authorising Officer”** means a person designated for the purposes of the

2000 Act to grant authorisations for directed surveillance. (see the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order) SI 2000/2417.

Note A. *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.*

Note B. *Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

Notification to Central Register of Authorisations under RIPA

Whether it is for Directed Surveillance or CHIS	
Applicants name and Job Title (manager responsible)	
Service and Section	
Applicant's address and Contact Number	
Identity of 'Target'	
Authorising Officer and Job Title; (in line with delegation scheme)	
Date of Authorisation	
Whether confidential information is likely to be reviewed as a consequence of the investigation/operation	
The date the authorisation was cancelled	
Whether the authorisation is renewed.	

A copy of the authorisation shall also be sent (See above, Paragraph 9.2).

A unique reference number for the investigation or operation will be allocated by the Legal and Democratic Services Manager upon receipt of this notification. This reference must be used in subsequent correspondence regarding this authorisation.

APPENDIX 3

**Chief Operating Officer
Head of Paid Service
and Returning Officer**

Jacqui Sinnott-Lacey **

**Corporate Director
of Place and
Community**

Heidi McDougall *

**Corporate Director
of Transformation
and Resources**

Chris Twomey *

**Legal and
Democratic
Services Manager
Monitoring
Officer**

**Senior
Responsible
Officer**

Kay Lovelady

Supported by

**Assistant Solicitor
RIPA
Co-ordinator and
SPOC
Co-ordinator**

Judith Williams

* Authorising Officer

** Authorisations when knowledge of confidential information likely to be acquired or vulnerable individual or juvenile is to be used as a source.

The Office of Surveillance Commissioner's Guidance

Covert surveillance of Social Networking Sites (SNS)

The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).