APPENDIX A

Halton Borough Council
Regulation of Investigatory Powers Act 2000
Policy Document

INTRODUCTION

The Regulation of Investigatory Powers Act 2000 ("RIPA") introduced wide ranging controls over a number of investigatory powers exercised by public authorities. Local authorities may not exercise all of the powers covered by RIPA. This Policy covers the investigatory powers exercised (or exercisable) by local authorities such as Halton Council.

These investigatory powers are:

1. The use of covert human intelligence sources ("CHIS");

2. Covert Surveillance (specifically, directed surveillance);

3. Acquisition and disclosure of communications data.

All of these investigatory powers are the subject of detailed guidance in the form of Codes issued by the Home Office. There is also secondary legislation to supplement the requirements of RIPA together will additional guidance (and requirements) issued by the Investigatory Powers Commissioners Office (IPCO) – formerly, so far as relevant here, the Office of Surveillance Commissioners (OSC) and the Interception of Communications Commissioner's Office (IOCCO).

The purpose of this Policy is not to repeat or summarise the above information. Its purpose is;

- To set out the Council's approach to RIPA;
- To outline the relationship of the Council with external inspection agencies.

- To explain to the public where they may find out more about RIPA.

This Policy aims to improve the understanding and conduct of RIPA.

This Policy should be read together with the Council's Employees' Guide to Directed Surveillance & Use of Covert Human Intelligence Sources (CHIS).

THE COUNCIL'S APPROACH TO RIPA

The Council is committed to following RIPA in accordance will all of the relevant codes and guidance.

This commitment is manifested in the selection of various categories of authorised persons together with ensuring proper training for all those involved with RIPA.

The Council is also committed to giving full co-operation to the external inspection agencies described in this Policy.

The RIPA procedures are subject to change and the Council will keep its procedures under review to ensure continued compliance.

Authorised persons

The Council's Constitution states the follows:

SO 28a	**RIPA Authorising Officers/Designated Persons involving employment of juveniles or vulnerable CHIS or the acquisition of confidential information**	**Chief Executive or in his absence SD-C&R and SD-P&E**

SO 28b	**RIPA Authorising Officers/Designated Persons except in respect of 26a matters**	**Chief Executive Group Solicitors**
SO 28c	**Senior Responsible Officer** **RIPA Co-ordinator**	**OL-LD** **Practice Co-ordinator - Legal Services**

The Authorising Officers/Designated Persons[1], Senior Responsible Officers and RIPA Co-ordinator are all the appropriate level within the Council to undertake the relevant duties. The OL-LD is also the Council's Monitoring Officer.

The Constitution incorporates a reference to the independent requirement set out at the IOCCO Circular dated 1st June 2014. Whilst this refers to the acquisitions and disclosure of communications data it has also been adopted generally for RIPA activities.

The Council's Group Solicitors will be the 'lead' Authorising Officers/Designated Persons. Neither the Chief Executive nor the Strategic Directors of the Council would be expected to be familiar with the detailed RIPA procedures and would take advice from a Group Solicitor before acting on a request involving RIPA.

Exercise of delegated powers under SO28a (or by the Chief Executive under SO28b) would be expected to be extremely rare. In the vast majority of cases it would be expected that the Group Solicitor would act as Authorising Officer/Designated Persons.

[1] Different terminology is used for directed surveillance and acquisition and disclosure of communications data.

Training

The Council is a member authority of the National Anti-Fraud Network ("NAFN") and takes advantage of its training resources. The Council will also ensure that the internal training is carried out as appropriate.
The core requirements of training will focus on the "5 Ws" (who, what, where, when and why) together with the necessity and proportionality of any proposed action.

EXTERNAL INSPECTION AGENCIES

Office of Surveillance Commissioners (OSC)

The Office of Surveillance Commissioners is responsible for overseeing the use of covert surveillance by designated by designated public authorities. It does not oversee the intelligence or security services. The OSC is judge-based and entirely independent of Government and all other public authorities. Its aim is to provide effective and efficient oversight so that the conduct of covert activities by public authorities is human rights compliant in accordance with relevant legislation. With regard to the activities of the Council the OSC are the inspectors of the Council's actions related to directed surveillance and the use of covert human intelligence sources (CHIS).

Interception of Communications Commissioner's Office (IOCCO)

The function of the IOCCO is to keep under review the interception of communications and the acquisition and disclosure of communication data by intelligence agencies, police forces and other public authorities.

The IOCCO undertakes a range of different types of inspection by the primary type of inspection so far as the Council is concerned are communications data inspections. The primary objectives of inspections are to ensure that:

- the system in place for acquiring communication data are sufficient for the purposes of the Act that all relevant records have been kept;

- all acquisitions of communications data has been carried out lawfully and in accordance with Part 1 Chapter II and its associated Code of Practice
- the data acquired was necessary and proportionate to the conduct authorised;
- errors are being 'reported' or recorded and that the systems are reviewed and adapted in the light of any exposed weaknesses or faults.
- persons engaged in the acquisitions of data are adequately trained and are aware of the relevant parts of the legislation.

A separate policy document has been issued on the Investigatory Powers Act 2016 which was brought into force in early June 2019. This Act sets out the extent to which certain investigatory powers (relating to the acquisition of communications data from a telecommunications operator) may be used to interfere with privacy.

FINDING OUT MORE ABOUT RIPA

The primary link to RIPA information is: https://www.gov.uk/search?q=ripa

Investigatory Powers Commissioners Office (IPCO) https://www.ipco.org.uk/

The Council's Employees' Guide to Directed Surveillance and CHIS can be found on the Council's website.

Halton Borough Council

Regulation of Investigatory Powers Act 2000

Employees' Guide to Directed Surveillance & Use of Covert Human Intelligence Sources (CHIS)

Mark Reaney

Senior Responsible Officer

1 Introduction and 2012 Changes

1.1 The Regulation of Investigatory Powers Act 2000 (the 2000 Act), also known as RIPA, regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively. This Guidance should be read together with the Council's 'RIPA Policy'.

1.2 Halton Borough Council is therefore included within the 2000 Act framework with regard to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources.

1.3 The purpose of this Guidance is to:

1.3.1 explain the scope of the 2000 Act and the circumstances where it applies

1.3.2 provide guidance on the authorisation procedures to be followed.

1.4 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this Guidance and each Department should hold copies to which staff can refer.

1.5 In summary the 2000 Act requires that when the Council undertakes "Directed Surveillance" or uses a "Covert Human Intelligence Source" (CHIS) these activities must only be authorised by an officer *designated for that purpose* when the relevant criteria are satisfied.

1.6 The officers listed in Schedule 1 are the Council's Authorising Officers for the purposes of the Act. Such nomination permits officers to grant authority for any purpose (except authorising juveniles or vulnerable CHIS or the acquisition of confidential information — reserved to Chief Executive or in his absence the Strategic Directors).

1.7 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 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.

1.8 It should be noted that the Council cannot authorise "Intrusive Surveillance".

1.9 Authorising Officers and investigators within the Council are to note that the 2000 Act does not extend powers to conduct Intrusive Surveillance. Investigators should familiarise themselves with the provisions of Sections 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. Paragraph 2.4 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 Senior Responsible Officer. However, it is always safer to get authorisation.

1.11 Only the Chief Executive has the power to authorise directed surveillance involving the covert filming of any Council member or employee. Only the Chief Executive has the power to authorise the use of a minor as a covert human intelligence source.

1.12 From 1 November 2012 the Council is required to obtain approval from a Justice of the Peace prior to using **Directed Surveillance** or **CHIS** under the 2000 Act. Authorisations and notices under the 2000 Act will only take effect once an Order has been granted by a Justice of the Peace allowing the Council to undertake such surveillance.

1.13 Council use of Directed Surveillance under the 2000 Act will be limited to the investigation of crime which attracts a 6 month or more custodial sentence, with the exception of offences relating to the under-age sale of alcohol and tobacco. This is the Crime Threshold.

1.14 The Crime Threshold shall not apply to the use of Covert Human Intelligence Source (CHIS).

1.15 The changes introduced in November 2012 are further described within Home Office guidance the link to which can be found in Schedule 2 below.

1.16 References in this Guidance to 'authorisation' by officers are to be read in light of the above guidance. The authorisation in respect of Directed Surveillance can now only be given by a Justice of the Peace and applications must only be made via Halton Borough Council Legal Services who should also be consulted for advice.

2 Directed Surveillance

2.1 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.

2.2 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 in 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.

2.3 Intrusive Surveillance

2.3.1 Intrusive 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.

2.4 Before any officer of the Council (including Authorising Officers) 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.

2.4.1 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 apply.

2.4.2 Is it for the purpose of a specific investigation or a specific operation?

For example, are Town Hall 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, this would be categorised as a specific operation and will require authorisation.

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

Private information" includes any information relating to a person's private or family life.
For example, if part of an investigation is to observe an employee'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. If in doubt, it is safer to get authorisation

2.4.4 Is it 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.

2.4.5 **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.

3. Covert use of Human Intelligence Source

3.1 A person is a Covert Human Intelligence Source (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) as set out below.

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

c) he is a member of the public giving information which he is not tasked to do so but which he covertly passes to the Council in the course of a personal or other relationship. This may include repeat information being provided by the informant about a suspect or about a family with the information being provided during the course of a family or neighborhood relationship. Any such instances should be referred to the Senior Responsible Officer for further legal advice/clarification

3.2 The point made at 3.1 c) above merits further explanation. A member of the public giving information, albeit not tasked to do so, may nevertheless 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. Though it may be unlikely that the Council will make a CHIS authorisation, it is important that officers be alert to the risk that such an informant would in reality be a CHIS. 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. This is an example of 'status drift' where an informant who has been treated as not being a CHIS can cross over to being a CHIS. Officers must refer any such instance for legal advice before acting on the information received from such an informant.

3.3 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.

3.4 The above clearly covers the use of professional witnesses and members of the public to obtain information and evidence as well as the use of Council Officers.

4. Authorisations, Renewals & Duration

4.1 The Requirements for obtaining Authorisation

4.1.1 *Directed Surveillance*

4.1.1.1 For Directed Surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

a) that an authorisation is “necessary” (as set out within the Covert surveillance and covert human intelligence sources codes of practice); and

b) the authorised surveillance is “proportionate” to what is sought to be achieved by carrying it out such surveillance.

4.1.1.2 An authorisation is necessary if it is for the purpose of preventing or detecting crime.

4.1.1.3 The onus is therefore on the person authorising such surveillance to satisfy themselves it is:

a) necessary for one of the grounds referred to above and;

b) proportionate to its aim.

4.1.1.4 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained and correct up to date forms used. 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.

4.1.2 *Covert Use of Human Intelligence Sources*

4.1.2.1 The same principles as Directed Surveillance apply. (see paragraph **4.1.1.2** above)

4.1.2.2 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.

4.1.2.3 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.

4.1.2.4 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.

4.1.2.5 There will be a need to designate a handler, controller and record keeper in any CHIS authorisation

4.2 Requirements of the 2000 Act

4.2.1 In all cases, authorisations must be in writing. Officers must direct their mind to the circumstances of the individual case with which they are dealing when completing the form. Care must be taken to avoid the use of obsolete forms. The best way to achieve this is not to stockpile forms and download them when needed from the Gov.Uk webpage. The standard forms which must be used may be found using the links to the webpage In Schedule 2 below. When completing the forms Authorising Officers must set out details of what they are authorising (applying their minds to the "5 Ws ": namely, who, what, where, when and why), and their assessments of its necessity and proportionality.

4.2.2 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.

4.2.3 Authorisations lapse, if not renewed:
- 12 months - from date of last renewal if it is for the conduct or use of a CHIS; or- in all other cases (i.e. Directed Surveillance) 3 months from the date of their grant or latest renewal.

4.2.4 Any person entitled to grant a new authorisation can renew an existing authorisation in the same terms at any time before it ceases to have effect. But, for the conduct of a CHIS, an Authorised Officer should not 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 CHIS, the tasks given to them and information obtained

4.2.5 The benefits of obtaining an authorisation are described in paragraph 8 below.

4.2.6 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. In this context 'necessary' includes consideration of why the use of covert surveillance is 'necessary' in the particular investigation.

4.2.7 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.

4.2.8 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. In this context the judgement on 'proportionality' the Authorising Officer must have regard to:

a) whether it is proportionate to the matter being investigated;

b) whether it is proportionate to the degree of intrusion on the target and others; and

c) have reasonable alternative means of acquiring evidence been considered and discounted?

4.2.9 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.

4.2.10 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

4.2.11 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, or where there are special sensitivities.

Spiritual Counselling

4.2.12 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

4.2.13 The 2000 Act does not provide any special protection for 'confidential material'. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under the relevant Home Office Code. In cases where the likely consequence of the surveillance or the conduct of a CHIS would be for any person to acquire knowledge of a confidential nature, the carrying out of the surveillance or the deployment of the source should be subject to special authorisation. In these cases, the authorising officer should be the Chief Executive or one of the Strategic Directors nominated by the Council as an Authorising Officer for the purposes of the 2000 Act.

4.2.14 In general, any application for an authorisation which is likely to result in the acquisition of confidential information 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.

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

a) 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 Senior Responsible Officer before further dissemination takes place;

b) Confidential material should not be retained or copied unless it is necessary for a specified purpose;

c) Confidential material should be disseminated only where an appropriate officer (having sought advice from the Senior Responsible Officer) is satisfied that it is necessary for a specific purpose;

d) 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.

e) Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

Combined authorisations

4.2.16 A single authorisation may combine two or more different authorisations under the 2000 Act. Combined authorisations must not include intrusive surveillance activity.

4.2.17 In cases where the Council is acting on behalf of another agency (or vice versa), it is usually for the tasking agency to

obtain or provide the authorisation. For example, where surveillance is carried out by the Council on behalf of the Police, authorisations would be sought by the Police and granted by the appropriate authorising officer. Council staff must always obtain the prior approval of their relevant Chief Executive or Strategic Director before carrying out an investigation on behalf of another agency.

Handling and disclosure of product

4.2.18 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 4.2.15 above.

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

4.2.21 Authorising Officers must ensure that the relevant details of each authorisation are sent to the Senior Responsible Officer via the RIPA Co-ordinator as described in paragraph 6 below.

4.2.22 Applications and authorisations for directed surveillance or the use of a CHIS should be retained by the Authorising Officer, for a period of 3 years. 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.

4.2.23 Authorising officers must ensure compliance with the appropriate data protection requirements and the safeguards

set out in relevant codes of practice on the handling, dissemination, copying, storage and destruction of material.

4.2.24 The Authorising Officers shall schedule for deletion any information obtained through surveillance and all copies, extracts and summaries which contain such material as soon as they are no longer needed for an authorised purpose and, where criminal proceedings have resulted, in accordance with the Council's Retention Policy. Such information shall be held separately in a clearly labelled folder with a known retention period and thereafter securely destroyed.

4.2.25 Where material is obtained by surveillance or the use of a CHIS, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

4.2.26 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 Directed Surveillance or the use of a CHIS and, otherwise than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

4.3 Special Factors relating to the Use of CHIS

4.3.1 The Council will, on occasions, use an external or professional source for the purpose of obtaining information. It is also possible, though unlikely, that the role of a Council employee may be that of a CHIS.

4.3.2 Nothing in the 2000 Act prevents material obtained by an employee or someone else acting as a CHIS being used as evidence in court proceedings.

4.3.3 The Authorising Officer must consider the safety and welfare of anyone acting as a CHIS and the foreseeable consequences to others of the tasks they are being 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 CHIS, even after cancellation of the authorisation, should also be considered.

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

4.3.5 Before authorising the use of a CHIS, 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.

4.3.6 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.

4.3.7 Additionally, the Authorising Officer should make an assessment of any risk to a person acting as a CHIS in carrying out the proposed authorisation.

5 Covert surveillance of Social Networking Sites (SNS)

5.1 This topic is referred to as “online covert activity” in the August 2018 Code of Practice on Covert Surveillance and Property Interference (at paragraphs 3.10 to 3.17). A related but separate topic is the Investigatory Powers Act 2016 which deals with the acquisition of communications data from a telecommunications operator or a postal operator. Separate guidance is issued on that topic.

5.2 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.

5.3 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.

5.4 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).

5.5 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.

5.6 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).

Social media and directed surveillance.

5.7 The following procedure has been established to be compliant with OSC Guidance.

First Visit to a social media account

When a complaint is initially received the first visit to the social media account is to confirm whether or not criminality is taking place – at this point no data is captured.

Second Visit to a social media account

Simple Investigation – No Monitoring Required

If there is evidence of criminality a second visit is scheduled which will result in the capture of sufficient visual evidence to prove the criminality. The evidence captured on this occasion will be used to request a directed surveillance operation, an entry warrant at the Magistrates. N.B. The capture of data should only relate to the criminality in question.

a) Complicated Investigation – Further Monitoring Required

The evidence captured on this occasion can be used to request a directed surveillance/CHIS* operation, an entry warrant or both. Where the investigation requires further evidence from the social media account a directed surveillance authorisation must be obtained before further monitoring (visits to the account) are made.
* In the event a CHIS authorization is obtained it is not necessary to obtain a separate directed surveillance authorisation, as the requirements of this can be detailed I the CHIS authorisation.

6 Central Register of Authorisation

6.1 The 2000 Act requires a central register of all authorisations to be maintained. The Senior Responsible Officer or a nominated

representative maintains this register. The nominated officer is the RIPA Co-ordinator.

6.2 Whenever an authorisation is granted the Authorising Officer must arrange for the following details to be forwarded to the RIPA Co-ordinator or nominated representative:

Whether it is for Directed Surveillance or CHIS;
The unique reference number of the investigation;

- Applicants name and Job Title;
- Department and Division;
- Applicant's address and Contact Number; - Identity of 'Target';
- Whether confidential information is likely to be obtained;
- Authorising Officer and Job Title; (in line with delegation scheme)
- Date of authorisation;
- The date the authorisation was cancelled.

6.3 It is each Department's responsibility to securely retain a copy of all authorisations within their departments.

The original copy of the authorisation shall be forwarded to the Senior Responsible Officer for retention within the Central Records Register.

6.4 A chart illustrating the authorization process can be found in Schedule 3.

7 Codes of Practice

The Home Office has issued codes of practice that expand on this Guidance and copies are held by the Senior Responsible Officer for access by the public.

The codes do not have the force of statute, but are admissible in evidence in any criminal 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.
Further Guidance is issued by the Information Commissioner's Office (ICO).
Schedule 2 below provides links to relevant web addresses.

8 Benefits of Obtaining Authorisation under the 2000 Act.

8.1 The 2000 Act states that if an 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" and the benefits set out at paragraph 8.3 below will apply.

8.2 However, if you do not obtain the 2000 Act authorisation it does not, of itself, make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits incidental to any conduct that is lawful by virtue authorisation.

8.3 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 which is lawful by virtue of 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.

9 Scrutiny and Tribunal

9.1 To effectively "police" the 2000 Act, Commissioners regulate conduct carried out thereunder. The Chief Surveillance 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 those authorising Directed Surveillance and the use of a CHIS.

9.2 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, amongst 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.

SCHEDULE 1 – AUTHORISING OFFICERS AND OTHER ROLES

For the purposes of the Covert surveillance and covert human intelligence sources codes of practice, the person in a public authority responsible for granting an authorisation will be referred to as the "authorising officer".

The Following officers have been designated as authorising officers for the purpose of the Regulation of Investigatory Powers Act 2000. In the Council's Constitution these are referred to as Designated Persons.

A. Officers who may grant authorisation for the employment of juveniles or vulnerable CHIS or the acquisition of confidential information:

   Chief Executive or in his absence:-

   Strategic Director – Enterprise, Community and Resources

   Strategic Director – People

B. Officers who may grant authorisations under the Act across all Council Departments and Divisions (except for the employment of juveniles or vulnerable CHIS or the acquisition of confidential information):-

   Chief Executive

   Group Solicitor (Environmental and Licensing)

   Group Solicitor (Policy and Regeneration)

   Group Solicitor (Social Care and Education)

The above designations are subject to the independence requirements of the ICCO Circular of 1st June 2015.

Senior Responsible Officer & RIPA Co-ordinator

In addition to the above designations there are two other roles set out in the Council's Constitution.

The **Senior Responsible Officer** is the Operational Director (Legal and Democratic Services). The **RIPA Co-ordinator** is the Practice Co-ordinator Legal Services.

The above job tiles and associated duties and authorisations shall extend to posts that have succeeded the above posts as a result of internal reorganisations.

The role of the Senior Responsible Officer shall also include:-

- Training of all staff dealing with RIPA (including Authorisation Officers)
- Keeping officers up to date with practice and legal changes to RIPA legislation maintaining all documentation relating to RIPA (including the Council's RIPA Policy and this Guidance, Central Records Register, Authorisations etc);

SCHEDULE 2 - Useful RIPA Links

Regulation of Investigatory Powers Act 2000

http://www.legislation.gov.uk/ukpga/2000/23/contents

(Note that the above link does not include all subsequent amendments)

RIPA Codes

https://www.gov.uk/search?q=ripa

RIPA Forms

https://www.gov.uk/government/collections/ripa-forms--2

Home Office Guidance to Local Authorities on the 2012 Changes

https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

Investigatory Powers Commissioners Officer (IPCO)

https://www.ipco.org.uk/

SCHEDULE 3 Authorisation Process:-