# CORPORATE SURVEILLANCE GUIDANCE

# THE REGULATION OF INVESTIGATORY POWERS ACT 2000

**November 2018**

# Contents

# 1. INTRODUCTION

## 1.1 Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') brought into force the regulation of covert investigation by a number of bodies, including local authorities. RIPA regulates a number of investigative procedures, the most recent of which is the access to communications data. This document is intended to provide officers with guidance on the use of covert surveillance, Covert Human Intelligence Sources ('Sources') and the obtaining and disclosure of communications data under RIPA. Officers must take into account the Codes of Practice issued under RIPA

RIPA and the Codes of Practice may be found at:

https://www.legislation.gov.uk/ukpga/2000/23/contents
https://www.gov.uk/government/collections/ripa-codes

## 1.2 Background

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of a citizen, his home and his correspondence. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:

(a) in accordance with the law
(b) necessary (as defined in this document); and
(c) proportionate (as defined in this document)

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Senior Solicitor.

Each officer of the Council with responsibilities for the conduct of investigations, shall, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

The Senior Solicitor* is appointed as the senior responsible officer to ensure the integrity of the process within the Council and its compliance with RIPA; to have oversight of reporting of errors to the relevant oversight commissioner; responsibility for engagement with the office of Surveillance Commissioners when they conduct their inspections and where necessary, oversight of the implementation of any post-inspection action plan. The senior responsible officer will also ensure that Elected Members regularly review the Council's use of RIPA, including by the submission of an annual report to the Audit and Governance Committee detailing any trends,

concerns or other developments. The Leader of the Council will also be appraised of any relevant matters as and when they occur.

*on an interim basis from 1/9/18 – 31/12/18 this role will be covered by the HR Manager

## 1.3 Review

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to surveillance. This document will, therefore be kept under yearly review by the Senior Solicitor. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Senior Solicitor at the earliest possible opportunity.

## 1.4 Scope

RIPA covers the authorisation of directed surveillance, the authorisation of sources and the authorisation of the obtaining of communications data. Communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, contents of e-mails or interaction with websites. The use of the internet, and in particular social media/networking websites, to gather information prior to or during an operation may amount to directed surveillance. Although such information may be publically available, repeat or particularly detailed viewing of individual 'open source' sites for the purposes of intelligence gathering and data collection may require RIPA authorisation. An authorisation under RIPA will provide lawful authority for the investigating officer to carry out surveillance.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the General Data Protection Regulations 2018. RIPA forms should be used where **relevant** and they will only be relevant where the **criteria** listed on the forms are fully met.

# 2. GENERAL

## 2.1 Definition of 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.

Surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

## 2.2 Confidential Material

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential

information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential journalistic material and communications between an MP and a constituent.

Applications in which the surveillance is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The Authorising Officer shall give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

Where a likely consequence of surveillance would result in the acquisition of confidential material, the investigating officer must seek authority from the Head of Paid Service, or, in her absence, the Senior Solicitor.

The use or conduct of a covert human intelligence source to obtain matters subject to legal privilege must be subject to prior approval by the Surveillance Commissioner.

## 3. DIRECTED AND INTRUSIVE SURVEILLANCE

### 3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or 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 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 under RIPA to be sought for the carrying out of the surveillance.

### 3.2 Intrusive Surveillance

That surveillance becomes intrusive if the covert surveillance:

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; or
b) is carried out without that device being present on the premises or in the vehicle, is not intrusive unless 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, or
c) is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations

Therefore 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 surveillance device OR when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

For intrusive surveillance relating to residential premises or private vehicles, if any device used 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.

Where covert surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

The Council has no statutory powers to interfere with private property, and if there is any possibility of trespass occurring in the course of surveillance, advice should be sought from the Senior Solicitor as soon as possible.

Currently, local authorities are **not** authorised to carry out intrusive surveillance.

## 4. IDENTIFYING DIRECTED SURVEILLANCE

**Ask yourself the following questions:**

### 4.1 Is the surveillance covert?

Covert surveillance is any surveillance that 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.

If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, Officers will be behaving in the same way as a normal member of the public (eg in the case of most test purchases), and/or will be going about Council business openly (eg a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen eg where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that conditions are being met.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

Use of body worn cameras will be overt. Notification will be worn by officers stating body cameras are in use and it will be announced that recording is taking place. In addition, cameras will only be switched on when recording is necessary – for example, when issuing parking tickets.

### 4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although the provisions of the Act do not normally cover the use of overt CCTV surveillance systems or ANPR systems that monitor traffic flows or detect motoring offences, since members of the public are aware that such systems are in use, there may however be occasions when public authorities use overt CCTV or ANPR systems for the purposes of a specific investigation or operation. For example, if the

CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary. The Surveillance Camera Code of Practice provides further good practice guidance and can be found at: https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

### 4.3 Is the surveillance 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. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

### 4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

## 5. COVERT HUMAN INTELLIGENCE SOURCES

### 5.1 Definition

A person is a source if:

a) he establishes or maintains a personal or other relationship with a person, including establishing a 'legend' or cover profile, for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

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

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

A source may include those referred to as agents, informants and officers working undercover.

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 the purpose.

A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

This covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

The use or conduct of a source to obtain knowledge of matters subject to legal privilege must be subject to the **prior approval of the Surveillance Commissioner**.

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (eg walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

The Code of Practice states that the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

An authorisation under RIPA will provide lawful authority for the use of a source.

## 5.2 Security and Welfare

Only the Head of Paid Service or, in her absence, the Senior Solicitor is able to authorise the use of vulnerable individuals and juvenile sources. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, more particularly set out in the Covert Human Intelligence Source Code of Practice at https://www.gov.uk/government/collections/ripa-codes

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

# 6. Communications Data

## 6.1 Definition

This covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data.

For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

Communications data includes subscribers details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc.

Two types of data (Customer Data or Service Data) are available to local authorities and, when making an application for obtaining or disclosing such data, the applicant must specify exactly which type of information is required from within each of the subscriber data and service use data.

a) Customer data – (Subscriber data, RIPA s21(4))

Customer data is the most basic. It is data about users of communication services.

This data includes:

- Name of subscriber
- Addresses for billing, delivery, installation
- Contact telephone number(s)
- Abstract personal records provided by the subscriber (e.g. demographic information)
- Subscribers' account information – bill payment arrangements, including bank, credit/debit card details
- Other services the customer subscribes to.

b) Service data – (Service Use data, RIPA s21(4)(b))

This relates to the use of the service provider's services by the customer, and includes:

- The periods during which the customer used the service(s)
- Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers
- 'Activity', including itemised records of telephone calls (numbers called), internet connections, dates and times/duration of calls, text messages sent
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection
- 'Top-up' details for prepay mobile phones – credit/debit card, voucher/e-top up details

A third type of data (traffic data) is not accessible to local authorities.

# 7. SOCIAL NETWORKING SITES

## 7.1 Guidance

The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

*'The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.*

*The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).*

*In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.*

*As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.*

*Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.*

*Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.'*

## 8. AUTHORISATION PROCEDURE

### 8.1 General

Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale of alcohol or tobacco to underage persons.

Any officer who undertakes investigations on behalf of the Council shall seek provisional authorisation in writing from an Authorising Officer in relation to any directed surveillance or for the conduct and use of any source. Each provisional authorisation then needs to receive judicial approval before being acted upon.

Any officer wishing to engage in conduct in relation to a postal service and telecommunication system for obtaining communications data and the disclosure to any person of such data must also seek authorisation, the procedure and procedure of which differs slightly and is outlined in section 6.

### 8.2 Who can give Provisional Authorisations?

By law, the 'Authorising Officer' for local authority purposes is any assistant Chief Officer, assistant Head of Service, service manager or equivalent. An Authorising Officer may grant a provisional authorisation which does not take effect until it receives judicial approval. More senior officers within a Council may also give provisional authorisations in the circumstances to those whom they are senior. Please note that certain provisional authorisations, namely those relating to confidential information, vulnerable individuals and juvenile sources, can only be granted by the Head of Paid Service, or, in her genuine absence, the Senior Solicitor.

The Council's authorised posts are listed in Appendix 1. This appendix will be kept up to date by the Senior Solicitor and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, a request must be referred to the Head of Paid Service for consideration as necessary. The Head of Paid Service has the delegated authority to add, delete or substitute posts.

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the Senior Solicitor, before Authorising Officers are certified to sign any RIPA forms. A certificate of training will be provided to the individual and a central register of all those individuals who have undergone training

or a one-to-one meeting with the Senior Solicitor on such matters, will be kept by the Senior Solicitor.

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of any forms to the Senior Solicitor, the same are sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

## 8.3 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance.

An Authorising Officer shall not grant a provisional authorisation for the carrying out of directed surveillance, or for the use of a source or for the obtaining or disclosing of communications data unless (s)he believes:

a) that a provisional authorisation is necessary and
b) the provisional authorised investigation is proportionate to what is sought to be achieved by carrying it out

For local authority investigations, provisional authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing and detecting crime or of preventing disorder.

Conduct is not deemed "**proportionate**" if the pursuance of the legitimate aim listed above will not justify the interference or if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe. The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale of alcohol or tobacco to underage persons. Covert surveillance relating to dog fouling and similar matters will not be deemed a proportionate activity.

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities. Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

### 8.4 Collateral Intrusion

Before provisionally authorising investigative procedures, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for a provisional authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

### 8.5 Judicial Approval of Provisional Authorisations and Renewals

The Council is only able to grant a provisional authorisation or renewal to conduct covert surveillance. All provisional authorisations and renewals must be approved by the Magistrates Court before surveillance commences.

The Council must apply to the local Magistrates Court for an Order approving the grant or renewal of an authorisation. The Council does not need to give notice of the application to the person(s) subject to the application or their legal representatives. If the Magistrates Court refuse to approve the application, they may also make an order quashing the provisional authorisation.

The Magistrates will consider the provisionally authorised application or renewal, and will need to satisfy themselves satisfied that:

a) At the time of provisional authorisation, there were reasonable grounds for believing that the tests of necessity and proportionality were satisfied in relation to the authorisation, and that those grounds still exist;
b) That the person who granted provisional authorisation was an appropriately designated person;
c) The provisional grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under RIPA; and
d) Any other conditions provided for by an order made by the Secretary of State were satisfied.

### 8.6 Special Procedure for Provisional Authorisation of and Issuing of Notices in respect of Communications Data

The Act provides two different ways of provisionally authorising access to communications data; through a provisional authorisation under Section 22(3) and by a provisional notice under Section 22(4). A provisional authorisation would, following judicial approval, allow the authority to collect or retrieve the data itself. A provisional notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority serving the notice. An

Authorising Officer decides whether or not a provisional authorisation should be granted or a provisional notice given.

In order to illustrate, a provisional authorisation under Section 22(3), may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

Applications for the obtaining and disclosure of communications data may only be made by officers of the Council. Reference should be made to the process map at Appendix 2 for guidance as to the process to be followed.

Notices and, where appropriate, provisional authorisations for communications data must be channelled through a single point of contact ("SPoC") at the National Anti-Fraud Network ("NAFN"). The SPoC will independently scrutinise provisional applications, and advise authorising officers as to whether an authorisation or notice is appropriate.

The SPoC:

a) where appropriate, assesses whether access to the communications data is reasonably practical for the postal or telecommunications operator;
b) advises applicants and authorising officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators;
c) provides safeguards for authentication;
d) assesses the cost and resource implications to both the authorisation and postal or telecommunications operator.

Applications to obtain communications data should be made on the standard form at https://www.gov.uk/government/collections/ripa-forms--2 and submitted in the first instance to the SPoC, and if appropriate s/he will forward the application to a Designated Person for either the provisional authorisation of conduct or the provisional issuing of a notice. If satisfied that the proposed investigation is both necessary and proportionate, the Designated Person will, subject to judicial approval, return the authorisation or notice and associated judicial order to the SPoC who will then liaise with the postal / telecommunications company. The disclosure of data under a notice will be made to the SPoC.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the General Data Protection Regulations 2018 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

## 8.7 Urgency

Urgent authorisations are no longer available in relation to directed surveillance or covert human intelligence sources.

## 8.8 Standard Forms

All authorisations must be in writing.

Standard forms for seeking directed surveillance and source authorisations are provided at https://www.gov.uk/government/collections/ripa-forms--2. The authorisation shall be sought using the standard forms as amended from time to time.

## 9. ACTIVITIES BY OTHER PUBLIC AUTHORITIES

The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

## 10. JOINT INVESTIGATIONS

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (eg police, Customs & Excise, Inland Revenue etc):

(a) wish to use the Council's resources (eg CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, (s)he must obtain a copy of that agency's RIPA form for the record and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

## 11. DURATION, RENEWALS AND CANCELLATION OF AUTHORISATIONS

### 11.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed. Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source

b) three months from the date of judicial approval for directed surveillance

c) one month from the date of judicial approval for communications data, or earlier if cancelled under Section 23(8) of the Act.

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations cease to have effect (unless renewed or cancelled) after the designated time periods above.

### 11.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

Standard review forms for directed surveillance and CHIS are given at https://www.gov.uk/government/collections/ripa-forms--2 .

### 11.3 Renewals

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations

Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

A further requirement in relation to renewal of covert human intelligence sources, is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source

and for the purposes of making an Order, the Magistrates have considered the results of that review.

The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance and CHIS are given at https://www.gov.uk/government/collections/ripa-forms--2.

## 11.4 Cancellations

An Authorising Officer shall cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the authorising officer who issued it.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

Standard cancellation forms for communications data and cancellation forms for directed surveillance and CHIS are given at https://www.gov.uk/government/collections/ripa-forms--2.

## 12. RECORDS

The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in departments and a central register of all such forms will be maintained by the Senior Solicitor.

## 12.1 Central record of all Authorisations

The Senior Solicitor shall hold and monitor a centrally retrievable record of all provisional and judicially approved authorisations. The Authorising Officer must notify and forward a copy of any provisional notice or authorisation granted, renewed or cancelled and any judicial approval received or refused within 1 week of the event to the Senior Solicitor to ensure that the records are regularly updated. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners. These records will be retained for a period of at least three years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

The Senior Solicitor will monitor the submission of provisional and judicially approved authorisations and notices and give appropriate guidance, from time to time, or amend any provisional or draft document as necessary. The records submitted to the Senior Solicitor shall contain the following information:

a) the type of authorisation or notice
b) the date the provisional authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the date judicial approval was received or refused;
e) the unique reference number (URN) of the investigation or operation;
f) the title of the investigation or operation, including a brief description and names of subjects, if known;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;

h) whether the investigation or operation is likely to result in obtaining confidential information;

i) the date the authorisation or notice was cancelled.

## 12.2 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and a provisional authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification of the approval given by the Authorising Officer;

b) a record of the period over which the surveillance has taken place;

c) the frequency of reviews prescribed by the Authorising Officer;

d) a record of the result of each review of the authorisation or notice;

e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;

f) the date and time when any instruction was given by the Authorising Officer.

g) the unique reference number for the authorisation (URN)

Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

## 12.3 Other Record of Covert Human Intelligence Sources

Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant a provisional authorisation for the use or conduct of a source unless (s)he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

The records shall contain the following information:

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the Council;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source;

i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare

ii. have a general oversight of the use made of the source (not to be the person identified in (h)(i))

iii. have responsibility for maintaining a record of the use made of the source

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by the conduct or use of the source;

(m) any dissemination of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

## 13. RETENTION AND DESTRUCTION

**12.1** Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the council's policies and procedures currently in force relating to document retention. The following gives guidance on some specific situations, but advice should be sought from the Senior Solicitor where appropriate.

Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but retained in accordance with legal disclosure requirements.

Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

Material obtained in the course of an investigation may be used in connection with investigations other than the one that the relevant authorisation was issued for. However, the use or disclosure of such material outside the council, unless directed by any court order, should only be considered in exceptional circumstances, and in accordance with advice from the Senior Solicitor.

Where material obtained is of a confidential nature then the following additional precautions should be taken:

- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should only be disseminated in accordance with legal advice that it is necessary to do so for a specific purpose;
- Confidential material which is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person where to do so might prejudice the outcome of any civil or criminal proceedings;

- Confidential material should be destroyed as soon possible after its use for the specified purpose.

If there is any doubt as to whether material is of a confidential nature, advice should be sought from the Senior Solicitor.

## 14. NON RIPA

Due to the changes brought about by the Protection of Freedoms Act 2012, there may be circumstances whereby it is necessary, and proportionate, to carry out covert surveillance for activities which do not meet the crime threshold set out above.

In such circumstances, staff must complete a non-RIPA form, setting out why such activity is necessary and proportionate and giving due consideration to any potential collateral intrusion

Non-RIPA forms must be authorised by the Senior Solicitor. However, if the activity relates to an investigation against a member of staff, authorisation must be provided by the HR Manager

## 15. CONSEQUENCES OF IGNORING RIPA

RIPA 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.**

Where there is interference 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 RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data 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.

## 16. SCRUTINY OF INVESTIGATORY BODIES

The Office or Surveillance Commissioners (OSC) has been established under RIPA to facilitate independent scrutiny of the use of RIPA powers by the investigatory bodies that are subject to it. The Commissioners will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at www.surveillancecommissioners.gov.uk

There is also a statutory complaints system welcomed by the Council. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from the OSC. The Council welcomes this external scrutiny. It expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

**IF IN DOUBT ADVICE MUST BE SOUGHT FROM THE SENIOR SOLICITOR**

## Appendix 1 - List of RIPA Authorised Officers

As of 1 September 2018, the following officers may grant authorisations:

| | |
|---|---|
| Jenny Wallace | Head of Paid Service |
| Staci Dorey | Solicitor |
| Steve Hearse | Strategic Manager (Resources) |
| Sarah Ayres | HR Manager |

## Appendix 2 - Process Map for Accessing Communications Data