



# **Regulation of Investigatory Powers Act 2000**

## **Joint Policy and Procedure**

<b>Introduction.....</b>	<b>1</b>
1. What is this document for and why is it needed? .....	1
2. What is meant by necessary? .....	1
3. What is meant by proportionate?.....	2
4. What is covered by the Regulation of Investigatory Powers Act 2000? .....	3
5. Why do we need to follow these rules? .....	3
6. What is the relevant legislation? .....	3
7. What is the Council's Policy on RIPA? .....	3
8. When will this document be reviewed?.....	4
9. Who is responsible for reviewing this document and the use of RIPA? .....	4
10. How do I find out more? .....	4
<b>Surveillance .....</b>	<b>5</b>
11. What is Surveillance? .....	5
12. What is Covert Surveillance?.....	5
13. What are Covert Human Intelligence Sources?.....	6
14. How can I obtain communications data? .....	7
<b>Procedures.....</b>	<b>8</b>
15. What is the procedure for obtaining authorisation under RIPA? .....	8
<b>The Senior Responsible Officer's Duties .....</b>	<b>9</b>
16. Who is the Senior Responsible Officer? .....	9
17. What are my duties?.....	9
<b>The Investigating Officer's Duties under RIPA. ....</b>	<b>10</b>
18. What do I need to do? .....	10
19. What do I need to consider?.....	10
20. How do I apply?.....	12
21. What if authorisation is urgent? .....	12
22. How long will an authorisation last for? .....	12
23. I now have my authority for surveillance, what else I should be aware of? .....	12
24. What do I do if circumstances change during the investigation? .....	13
25. Why are renewals important? .....	13
26. What should I do?.....	13
27. Why are cancellations important?.....	14
28. How do I cancel an authorisation?.....	14
<b>Authorising Officer Responsibilities under RIPA .....</b>	<b>15</b>
29. Who are the Authorising Officers? .....	15
30. What are my responsibilities?.....	15
31. What do I need to consider?.....	15
32. What do I do if I have refused the application?.....	16

33.	What do I do if I have approved the application? .....	16
34.	What do I do if the authorisation is urgent? .....	17
35.	What is the procedure for applying for Judicial Approval.....	17
36.	What do I do with the completed forms? .....	19
37.	How long will an authorisation last for? .....	20
38.	I have now given the authority for surveillance, what should I do next? .....	20
39.	Why are renewals important? .....	20
40.	What are my responsibilities in respect of renewals? .....	20
41.	What do I do with the completed form? .....	21
42.	Why are cancellations important?.....	22
43.	What are my responsibilities in respect of cancellations?.....	22
44.	What do I do with the completed form? .....	22
<b>Working with or through other Agencies .....</b>		<b>23</b>
45.	What do I do if I want to instruct another organisation to carry out surveillance? .	23
46.	What do I do if I want to carry out an investigation with another organisation? ....	23
<b>Record-Keeping .....</b>		<b>23</b>
47.	What records must I keep?.....	23
48.	How long must I keep these records? .....	23
49.	How should the records relating to a CHIS be maintained? .....	23
50.	How should material be handled and stored? .....	24
51.	What about confidential material? .....	24
<b>Complaints .....</b>		<b>24</b>
52.	Is there a complaints procedure in place? .....	24
<b>Annex A .....</b>		<b>25</b>
<b>Annex B .....</b>		<b>26</b>

## Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) means that formal authorisation from a senior officer must be obtained before carrying out certain surveillance, monitoring and other evidence-gathering activities. The Council may not carry out any other types of surveillance at all.

It is important to remember that RIPA must always be complied with, regardless of whether the information obtained is to be used as evidence in court proceedings. Failure to comply with RIPA doesn't just mean that the evidence cannot be used in court; it means that the whole procedure is illegal and that the officers concerned do not benefit from the above protection.

### 1. What is this document for and why is it needed?

1.1 Councils' are allowed and required to carry out investigations in relation to their duties. Such investigations may require surveillance or information gathering of a covert nature.

1.2 **Article 8** of the European Convention on Human Rights provides:

**Article 8.1:** Everyone has the right to respect for his private and family life, his home and his correspondence.

**Article 8.2:** There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society:

- In the interests of national security,
- Public safety or the economic well-being of the country,
- For the prevention of disorder or crime,
- For the protection of health or morals, or for the protection of rights and freedoms of others.

1.3 This right is not absolute, it is a qualified right. This means that in certain circumstances the Council *may* interfere with the right if the interference is:

- in accordance with the law
- necessary, and
- proportionate

1.4 Covert Surveillance and information gathering may constitute an interference with the right to respect for private and family life. To ensure that such an action is not unlawful under the Human Rights Act 1998, the Council needs to meet the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA).

1.5 In simple terms, RIPA requires the Council to have in place procedures to ensure that when required, surveillance is necessary and is properly authorised. Surveillance is usually a last resort that an investigator will use to prove or disprove an allegation. RIPA sets out a statutory mechanism for authorising covert surveillance and the use of covert human intelligence sources (see below). RIPA seeks to ensure that any interference with an individual's rights under Article 8 is necessary and proportionate and that, therefore, there is a balance between public interest and an individual's human rights. Covert surveillance will only be undertaken where there is no reasonable and effective alternative means of achieving the desired objective.

### 2. What is meant by necessary?

- 2.1 It is essential to consider whether an investigation requiring surveillance or information gathering can be done overtly rather than covertly. What would the result be if you carried out the investigation overtly?
- 2.2 If an investigation can be reasonably carried out by any means other than by using covert surveillance, then the use of covert surveillance is not necessary.
- 2.3 It must then be considered whether it is necessary to conduct covert surveillance or use covert human intelligence sources in the circumstances of the particular case for the purpose of preventing or detecting crime where the offence is punishable by imprisonment of a term of six months or more.

### **3. What is meant by proportionate?**

- 3.1 Proportionality is a key concept of RIPA. Any authorisation to carry out surveillance should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (i.e. 'a sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

You should make clear that the following elements of proportionality have been fully considered:

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
- providing evidence of other methods considered and why they were not implemented

The Authorising Officer should set out, in their own words, why they believe (RIPA) the activity is necessary and proportionate. Simply saying it is necessary is insufficient.

- 3.2 The use of surveillance must be designed to do no more than meet the objective in question; it must not be unfair or arbitrary, and the impact on the individual (or group of people) concerned must not be too severe. In deciding whether the use or action is proportionate, the risk of intrusion into the privacy of persons other than those who are the object of the investigation must be considered, and the measures proposed to minimise such intrusion must be properly assessed. You must be satisfied that, on balance, the principle of the subject's right to privacy is outweighed by the purpose of the investigation. Clearly, the more serious the matter being investigated, the more likely that surveillance will be proportionate.
- 3.3 The proportionality test will also require you to consider whether there are any other appropriate means of obtaining the information and whether there is a risk of collateral intrusion. The least intrusive method will be proportionate. Some of the things you may also wish to consider in terms of proportionality are whether covert surveillance is the only option, what other options have been considered, the intended length of the investigation, the number of officers to be deployed in the investigation.

- 3.4 The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

#### **4. What is covered by the Regulation of Investigatory Powers Act 2000?**

- 4.1 The main purpose of the Regulation of Investigatory Powers Act 2000 is to ensure that the relevant investigatory powers are used in accordance with human rights. The Act sets out these powers in more detail. Part II of the Act sets out the powers available to local authorities.
- 4.2 The Council is able to carry out investigations using covert surveillance and/or by using a covert human intelligence source under RIPA following the formal authorisation procedures and codes of practice as set out in this document. RIPA applies to the Council's core functions.
- 4.3 Please ask the RIPA Co-ordinating Officer for advice if you are unsure as to whether RIPA will apply.
- 4.4 RIPA not only covers the surveillance of members of the public but could also cover the observation of staff and members as part of an internal investigation.

#### **5. Why do we need to follow these rules?**

- 5.1 Following the requirements of RIPA and acting in accordance with this Policy, will protect the Council against potential challenges to its decisions and procedures. Not following the procedures specified in this document could also lead to a complaint of maladministration or a complaint to the independent Tribunal set up under RIPA, details of which are to be found at the end of this document.
- 5.2 The Council is also regularly inspected by a representative of the Investigatory Powers Commissioner's Office (IPCO) to ensure that all relevant legislation is complied with.

#### **6. What is the relevant legislation?**

- The Regulation of Investigatory Powers Act 2000
  - The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
  - Protection of Freedom Act 2012
  - Investigatory Powers Act 2016 (initiated the oversight role of the Investigatory Powers Commissioner)
- 6.1 Authorisation may only be granted if it is necessary for the reason permitted by RIPA. For local authorities the only statutory reason is **for the purposes of preventing or detecting a criminal offence where that offence is punishable (whether on summary or indictment) by a minimum term of at least 6 months imprisonment.**
- 6.2 This means that directed surveillance cannot be used for minor offences.

#### **7. What is the Council's Policy on RIPA?**

- 7.1 This document is the Council's policy on RIPA. As such, it should be adhered to unless it is in conflict with either of the Government Codes of Practice which have been made under RIPA. The Codes of Practice are admissible as evidence in court and **must** be complied with.
- 7.2 Copies of the Codes of Practice are available on the [Home Office website](#): These are:

- Covert Surveillance Code Of Practice
- Covert Human Intelligence Sources Code Of Practice

## **8. When will this document be reviewed?**

- 8.1 This document shall be subject to review every two years. An earlier review may take place should circumstances in the law so require it. Minor amendments may be made by the Monitoring Officer from time to time.

## **9. Who is responsible for reviewing this document and the use of RIPA?**

- 9.1 The Council's **Audit and Governance Committee** is responsible for the overview of the RIPA policy and the Councils' use of RIPA. The Committee will not be involved in making decisions on specific authorisations.
- 9.2 The RIPA Co-ordinating Officer is responsible for the RIPA Policy, the Central Register of authorisations, and for making regular reports on the use of RIPA to the Councils Audit and Governance Committee.

## **10. How do I find out more?**

- 10.1 General guidance on RIPA may be found on the [Home Office website](#):
- 10.2 Please contact the Council's Monitoring Officer if you require any further advice on RIPA, this document or any of the related legislative provisions.

## Surveillance

### 11. What is Surveillance?

#### 11.1 “Surveillance” includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications
- recording anything mentioned above in the course of authorised surveillance
- surveillance, by or with, the assistance of appropriate surveillance device(s)
- the interception of a communication in the course of its transmission by means of a postal service or telecommunication system if it is one sent by, or intended for, a person who has consented to the interception of the communication.

#### 11.2 Surveillance can be overt or covert.

#### 11.3 Overt Surveillance

Overt Surveillance is that which is not covert, the definition of which follows in section 12.1.

Overt surveillance does **not** require authorisation under RIPA.

### 12. What is Covert Surveillance?

#### 12.1 “Covert Surveillance” means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

**Covert surveillance does require authorisation under RIPA.**

#### 12.2 RIPA regulates two types of covert surveillance:

- Directed Surveillance, and
- Intrusive Surveillance;

#### 12.3 RIPA also regulates the use of Covert Human Intelligence Sources (see section 13)

#### 12.4 Directed Surveillance

Directed surveillance is defined as surveillance which is:

- covert,
- not intrusive (see definition below)
- undertaken for the purposes of a specific investigation or specific operation;
- carried out in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is the target of the investigation or operation); and
- undertaken in a planned manner, and not as an immediate response to events or circumstances.

#### 12.5 Use of the internet and social networking sites may potentially fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy).



12.6 The Chief Surveillance Commissioner has made specific reference to the increasing use of Social networking sites as a method of gathering intelligence and has stated in the Annual report:

‘Although there remains a significant debate as to how anything made publically available in this medium can be considered private, my commissioners remain of the view that the repeat viewing of individual ‘open source’ sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity.

There is a fine line between general observation, systematic observation and research and it is unwise to rely on a perception of a person’s reasonable expectations or their ability to control their personal data.’

12.7 The Council’s policy in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below:

- officers must not ‘friend’ individuals on social networks or set up fake profiles
- officers should not use their own private accounts to view the social networking accounts of other individuals
- officers viewing an individual’s profile on a social networking site should do so only once in order to obtain evidence to support refute their investigation
- further viewing of open profiles on social networking sites to gather evidence or to monitor an individual’s status, must only take place once RIPA authorization has been granted and approved by a Magistrate
- officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

#### 12.8 Intrusive surveillance

Intrusive surveillance is surveillance of any activities on any **residential premises** or in any private vehicle by a person (other than a Covert Human Intelligence Source) on those premises or in that vehicle or is carried out by means of a surveillance device on the premises or in the vehicle or which provides information of the same quality and details as if it was on the premises or in the vehicle

12.9 However, directed surveillance authorisation may be granted for parts of residential premises, such as gardens or driveways which can be observed from the public highway. Further guidance on this point may be obtained from the Council’s Monitoring Officer.

12.10 It is important to get this right because:

#### **COUNCIL OFFICERS CANNOT CARRY OUT INTRUSIVE SURVEILLANCE**

#### 12.11 Interference with property

Under RIPA, local authorities can not authorise any ‘interference with property’ activities. However, it may be necessary to conduct a minor trespass in order to conduct the covert surveillance which may have a civil liability implication for the Council. It is important that if such matters are considered appropriate legal advice is taken beforehand.

### 13. What are Covert Human Intelligence Sources?

13.1 The term Covert Human Intelligence Sources (CHIS) is used to describe people who are more commonly known as informants or officers working “undercover”.

13.2 This does not include members of the public who volunteer information to the Council as part of their normal civic duties or to contact numbers set up to receive information.

13.3 A person is a CHIS if he/she:

- establishes or maintains a covert personal or other relationship for the purposes of:
- obtaining information; or
- providing access to information to another person; or
- discloses information obtained by the use or existence of that covert relationship

13.4 RIPA authorisation is required for using a CHIS.

13.5 There are special rules for using juvenile or vulnerable persons as a CHIS, and only the Chief Executive can authorise such surveillance.

13.6 Further advice should be sought from the Council's Monitoring Officer in such cases.

#### **14. How can I obtain communications data?**

14.1 Local authorities can carry out interception of communications in a restricted number of circumstances.

These are:

##### **14.2 In the course of normal business practice**

The Councils are permitted without authorisation under RIPA to lawfully intercept its employees' e-mail or telephone communications and monitor their internet access for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems.

The Councils' policies on use of the internet and e-mail are set out on the Council's intranet.

##### **14.3 Interception with the consent of both parties.**

Such interception does not require RIPA authorisation, but should be properly recorded.

##### **14.4 Interception with the consent of only one of the parties.**

Such interception would require RIPA authorisation because it would fall within the definition of surveillance (either directed or using a CHIS). The main type of interception envisaged here is the recording of telephone calls where either the caller or the receiver has given consent to the recording.

Where as part of an already authorised Directed Surveillance or use of a CHIS a telephone conversation is to be recorded by the Officer or the CHIS then no special or additional authorisation is required.

##### **14.5 Interception without the consent of either of the parties**

The recording of telephone calls between two parties when neither party is aware of the recording **CANNOT BE UNDERTAKEN**, except under a Warrant granted by the Secretary of State under Part 1 of RIPA. Such warrants are only granted by the Secretary of State and it is not envisaged that such activity would fall within the remit of local authority investigations.

## **Procedures**

### **15. What is the procedure for obtaining authorisation under RIPA?**

15.1 Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

15.2 All directed surveillance and use of a CHIS operations shall be:

- Applied for in writing
- Authorised by a magistrates court
- Monitored
- Renewed by a magistrates court (when necessary)
- Cease when no longer authorised

15.3 All the above actions will be carried out in accordance with this document and the relevant Codes of Practice and will be recorded on the Standard Forms listed below:

15.4 The Standard Forms are available from the [Home Office web-site](#).

#### **15.5 Directed Surveillance**

- Application for directed surveillance authorisation
- Review of directed surveillance authorisation
- Application for cancellation of directed surveillance authorisation
- Application for renewal of directed surveillance authorisation

#### **15.6 Use of a Source**

- Application for conduct-use of a CHIS authorisation
- Review of use of a CHIS authorisation
- Application for renewal of use of a CHIS authorisation
- Application for cancellation of conduct-use of a CHIS authorisation

15.7 Copies of all these documents will be retained and kept on the investigation file as part of the evidence to show that the information gained by directed surveillance or the use of a CHIS has been obtained legally.

15.8 This document provides guidance on the Procedures required to be undertaken by the Investigating Officer and the Authorising Officer for the different stages specified above.

## **The Senior Responsible Officer's Duties**

### **16. Who is the Senior Responsible Officer?**

16.1 The Councils' Senior Responsible Officer is listed in the annex to this document.

### **17. What are my duties?**

In accordance with the recommendations of the Codes of Practice, you are responsible for the following areas:-

- The integrity of the process in place within the Council for the management of Covert Human Intelligence Sources and Directed Surveillance.
- Annual retrospective quality assurance review of all RIPA investigations undertaken
- Compliance with Part II of RIPA and the Codes of Practice.
- Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
- Engagement with the OSC inspectors when they conduct their inspections.
- Oversight of the implementation of any post-inspection action plan approved by the relevant oversight Commissioner.
- Ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports by the Office of the Surveillance Commissioner.

## **The Investigating Officer's Duties under RIPA.**

### **The Application**

**The application for authorisation is the responsibility of the Investigating Officer.**

#### **18. What do I need to do?**

18.1 You will need to consider:

- Whether covert surveillance is needed.
- Whether directed surveillance or use of a CHIS is needed.
- Whether directed surveillance or use of a CHIS is necessary for statutory reasons.
- Whether directed surveillance or use of a CHIS is proportionate.
- The risk of collateral intrusion.
- Safety and welfare arrangements (use of Source only).

These are discussed in more detail below.

#### **19. What do I need to consider?**

##### **19.1 Whether covert surveillance is needed**

Consideration must be given as to whether covert surveillance is needed. You are advised to discuss the need to undertake directed surveillance or the use of a CHIS with your line manager before seeking authorisation. All options for the use of overt means **must** be fully explored. Remember: if the investigation can be carried out by overt means, then covert surveillance is not necessary.

##### **19.2 Whether directed surveillance or use of a CHIS is needed**

You must establish which type of "surveillance" is required for the investigation or operation having regard to the guidance contained in this document. The type of surveillance you require affects which application forms you need to complete. Additional considerations are needed for using a CHIS. Further detail is found below. Combined authorisations for both directed surveillance and the use of a CHIS may be applied for where appropriate.

**Remember that sometimes the use of 'Social Media' may amount to a directed surveillance. If you are thinking of doing this, then please contact the Council's Monitoring officer for advice as to whether you require a RIPA authorisation.**

##### **19.3 Whether directed surveillance or use of a CHIS is necessary for the statutory reason**

Authorisation may only be granted if it is necessary for the reason permitted by RIPA.

For local authorities the only statutory reason is **for the purposes of preventing or detecting a criminal offence where that offence is punishable (whether on summary or indictment) by a minimum term of at least 6 months imprisonment.**

You must set out this ground in your application form and provide details of the reasons why it is necessary to use covert surveillance.

##### **19.4 Whether directed surveillance or use of a CHIS is proportionate**

You must consider why it is proportionate to use covert methods to collect evidence. Please see the definitions set out on page 2 "what is proportionate?" Remember, the use of covert

methods must do no more than meet your objective. The proportionality test will also require you to consider whether there are any other appropriate means of obtaining the information and whether there is a risk of collateral intrusion (see consideration below). The least intrusive method will be proportionate. The following aspects of proportionality must be considered and evidenced:-

- (a) Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- (b) Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
- (c) Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result
- (d) Evidencing, as far as reasonably practicable, what other methods have been considered and why these were not implemented.

#### **19.5 The risk of collateral intrusion**

Collateral intrusion is the risk of intrusion into the privacy of persons other than the target. You are required to assess the risk of collateral intrusion. Details of any potential collateral intrusion should be specified. Measures must be taken wherever practicable to avoid or minimise collateral intrusion and a plan should be included in your application specifying how the potential for collateral intrusions will be minimised. You should give as much detail as possible, insufficient information may lead to the rejection of the application.

#### **19.6 Surveillance from private premises**

It is preferable for surveillance to be carried out from a public place, such as a public highway. However, there may be circumstances where private premises may be required for the carrying out of surveillance. In which case, it is essential that you obtain the consent of the owner and/or occupier of the premises prior to authorisation being sought.

You should seek further guidance from the Council's Monitoring Officer on this point.

#### **19.7 Safety and welfare arrangements – use of a CHIS**

Before authorising the use of a CHIS you must ensure that a risk assessment is carried out to determine the risks to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing safety and welfare of the CHIS, after the cancellation of the authorization, should also be considered at the outset.

Details must also be included setting out the arrangements for the safety of the CHIS, this should include:

- (a) The name of the Officer who has day to day responsibility for:
  - Dealing with the CHIS.
  - Directing the day to day activities of the CHIS.
  - Recording the information supplied by the CHIS.
  - The CHIS's security and welfare.
- (b) The name of the Officer responsible for recording and monitoring the use made of the CHIS.
- (c) Arrangements for ensuring the security of the records which identify the CHIS.
- (d) Records relating to the CHIS meet the requirements of the Statutory Instrument: The Regulation of Investigatory Powers (Source Records) Regulations 2000

(SI 2000 No. 2725) – please see either the [Home Office website](#) or the [Office of Public Sector Information website](#).

## **20. How do I apply?**

20.1 All applications must be made in writing on the standard forms provided by the Home Office.

20.2 The relevant forms are:

- An application for directed surveillance authorisation, and/or
- An application for use of a CHIS.

20.3 The considerations set out above, form part of the application form.

20.4 The application form must be fully completed and passed to the Authorising Officer. The annex to this document contains details of the Council's Authorising Officers.

**NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.**

## **21. What if authorisation is urgent?**

21.1 The 2012 Home Office Guidance states that in most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. Therefore local councils may need to work with the police if faced with an emergency.

NB. Urgent authorisation may not be necessary if, under section 26(2) of the Act, an officer suddenly sees something relevant to his duties and takes an immediate note, observation of follow-up activity (within reason).

## **Monitoring**

## **22. How long will an authorisation last for?**

22.1 The authorisation for Directed Surveillance will last for **three months** from the date of authorisation unless renewed.

22.2 The authorisation for use of a CHIS will last for **12 months** from the date of authorisation (i.e. date of Magistrates' Order) unless renewed.

22.3 Review dates for the authorisation will be set by the Authorising Officer.

## **23. I now have my authority for surveillance, what else I should be aware of?**

23.1 It will be the responsibility of the Investigating Officer to ensure that any Directed Surveillance or use of a CHIS is only undertaken under an appropriate and valid authorisation. It is also important for you to ensure that those undertaking the surveillance have read the authorization and understand exactly what has been authorised.

23.2 During the surveillance, you should ensure:

- Surveillance is carried out in accordance with the approval
- Collateral intrusion is minimised as far as possible
- Intrusive surveillance is not carried out
- All information obtained is recorded contemporaneously or as soon as possible thereafter

23.3 During the use of a CHIS, you should also ensure that the CHIS is aware that:

- Only the tasks authorised are carried out
- Third party collateral intrusion is minimised as far as possible
- Intrusive surveillance is not carried out
- Entrapment is not committed
- They must regularly report to you

23.4 You should also be mindful of the date when authorisations and renewals will cease to have effect. Please see the notes on Renewals and Cancellation below.

## **24. What do I do if circumstances change during the investigation?**

24.1 You must inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation or if there is another change in circumstances usually brought about by unforeseen action.

24.2 When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised (for minor amendments only) or whether it should be cancelled and a new authorisation obtained. The relevant forms should be used.

24.3 Particular care should be taken when using a CHIS to ensure that authorisation is sufficient. It is difficult to predict what might occur each time a meeting with a CHIS takes place. If unforeseen action takes place, the occurrence should be recorded as soon as possible after the event and the sufficiency of the authorisation must be considered.

24.4 You must bring to the attention of the Authorising Officer any concerns about the personal circumstances of the CHIS in relation to: the validity of the risk assessment; the conduct of the CHIS; the safety and welfare of the CHIS.

## **Renewals**

## **25. Why are renewals important?**

25.1 Surveillance must cease unless a renewal has been applied for and approved. Renewals must be authorised prior to the expiry of the original authorisation but will run from the date and time of expiry of the original authorisation.

## **26. What should I do?**

26.1 If it appears that the directed surveillance or use of a CHIS is needed beyond the authorisation date, you must seek a renewal of the authorisation.

26.2 You must consider whether covert methods are still necessary and proportionate.

26.3 An application for renewal for either Directed Surveillance and/or use of CHIS should be made on the relevant form provided by the Home Office at [www.homeoffice.gov.uk](http://www.homeoffice.gov.uk) and passed to the Authorising Officer for consideration.

**NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.**

## **Cancellations**



## **27. Why are cancellations important?**

27.1 All authorisations, including renewals, must be cancelled if the reason why Directed Surveillance or use of a CHIS was required no longer exists or is no longer proportionate. This will occur in most instances when the purpose for which surveillance was required has been achieved and officers must be mindful of the need to cancel any authorisation which has been issued. A cancellation should be issued at the expiry date if not before.

## **28. How do I cancel an authorisation?**

28.1 To cancel an authorisation, you should complete the Cancellation of Authorisation form provided by the Home Office at [www.homeoffice.gov.uk](http://www.homeoffice.gov.uk) and submit it to the Authorising Officer for endorsement.

## Authorising Officer Responsibilities under RIPA

### The Approval

#### 29. Who are the Authorising Officers?

- 29.1 The Council's Authorising Officers are listed in the annex to this document.
- 29.2 If the investigation may involve the acquisition of confidential or religious material, or require an authorisation for using juveniles or vulnerable persons as sources, the Authorising Officer is, by law, the Chief Executive (or in his absence the Deputy Chief Executive).
- 29.3 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. If this is the case, the application form for authorisation should be noted to this effect.

**NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.**

#### 30. What are my responsibilities?

- 30.1 Responsibility for authorising the carrying out of directed surveillance or using a CHIS rests with the Authorising Officer and requires the personal authority of the Authorising Officer.
- 30.2 You must be satisfied that a defensible case can be made for surveillance. Authorisation is a safeguard against the abuse of power by public authorities. Full consideration of necessity and proportionality will make the action less vulnerable to challenge under the Human Rights Act 1998.

#### 31. What do I need to consider?

- 31.1 You are required to consider the application for authorisation in relation to the following:

**Is the directed surveillance or use of a CHIS necessary?**

- 31.2 **Firstly**, you must consider whether it is necessary to carry out the investigation by covert methods. This is an important consideration and must be recorded on the form. Please see "what is meant by necessary?" on Pages 1 and 2 of the Policy.
- 31.3 **Secondly**, as authorisation may only be granted if it is necessary for the reason permitted by RIPA. You should consider, having regard to the outline of the case provided by the Investigating Officer, whether authorisation is necessary for the purposes of preventing and detecting crime or of preventing disorder

**Is the directed surveillance or use of a CHIS proportionate?**

- 31.4 This involves balancing the intrusiveness of the activity on the target and others who may be affected by it (see "consideration: risk of collateral intrusion" below) against the need for the activity in operational terms. Please refer to "what is proportionate?" on page 2 of this Policy.

**Consideration: The risk of collateral intrusion**

- 31.5 You must take into account the risk of interfering with the privacy of persons other than the target (collateral intrusion). Full details of potential collateral intrusion and the steps to be taken to minimise such intrusion must be included in the form. If there are insufficient details further information should be sought. Collateral intrusion forms part of the proportionality test

and is therefore very important. Remember: the least intrusive method should be chosen otherwise the surveillance activity will not be proportionate.

#### **Consideration: confidential material**

- 31.6 In cases where through the use of directed surveillance or the use of a CHIS it is likely that knowledge of confidential information will be acquired, authorisation may only be granted by the Chief Executive.
- 31.7 Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.
- 31.8 Authorisation involving the acquisition of confidential information should only be given in exceptional and compelling circumstances having full regard to the proportionality issues involved.
- 31.9 Further details about the type of information covered under this category are to be found in the Chapter 3 of the relevant Code of Practice. Further advice may be sought from the Council's Monitoring Officer.

#### **Consideration: Safety and welfare arrangements of a CHIS**

31.10 When authorising the conduct or use of a CHIS, you must be satisfied:

- That the conduct and/or use of the CHIS is proportionate to what is sought to be achieved;
- That arrangements exist for the management and oversight of the CHIS, particularly the health and safety of the CHIS including:
  - Identifying the person who will have day to day responsibility for dealing with the CHIS
  - Security and welfare arrangements of the CHIS both during and after the investigation/operation.
  - Monitoring and recording the information supplied by the CHIS
  - Ensuring records disclosing the identity of the CHIS will not be made available to persons except where there is a need for access to them
  - Records relating to the CHIS meet the requirements of the Statutory Instrument: The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000 No. 2725) – please see either the [Home Office website](#) or the [Office of Public Sector Information website](#).

#### **Consideration: local community**

31.11 You should consider whether there any particular sensitivities in the local community where surveillance will be taking place.

**Having taken all these factors into consideration, you may either authorise the application or refuse it.**

### **32. What do I do if I have refused the application?**

32.1 You must complete the form and give your reasons for refusal. Then follow the procedures below ("I have completed the form what do I do with it?")

### **33. What do I do if I have approved the application?**

33.1 You need to follow the rest of the procedure set out below.

- 33.2 Regular review should be undertaken to assess the need for surveillance or use of a CHIS to continue and whether it is still proportionate. Where the surveillance or use of a CHIS provides access to confidential information or involves collateral intrusion, review should be more frequent.
- 33.3 You will therefore need to consider a Review Date(s). Both types of authorisation require you to specify a date when the authorisation should be reviewed (the Review Date) and the frequency of the review thereafter. This must be stated on the form.

#### **34. What do I do if the authorisation is urgent?**

- 34.1 The 2012 Home Office Guidance states that in most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. Therefore local councils may need to work with the police if faced with an emergency.

NB. Urgent authorisation may not be necessary if, under section 26(2) of the Act, an officer suddenly sees something relevant to his duties and takes an immediate note, observation of follow-up activity (within reason).

#### **35. What is the procedure for applying for Judicial Approval**

- 35.1 Following approval by you as the authorising officer the first stage of the process is for you to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.
- 35.2 You will need to provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration
- 35.3 The original RIPA authorisation or notice should be shown to the JP but should be retained by you so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). However, the court may wish to take a copy. In addition, you need to provide the JP with a partially completed judicial application/order form at Annex B.
- 35.3 Although you are required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.
- 35.4 The order section of this form will be completed by the JP and will be the official record of the JP's decision. You will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and you will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

#### **Arranging a Hearing**

- 35.5 You will need to contact HMCTS administration as soon as possible to request a hearing. On the rare occasions where out of hours access to a JP is required then it will be for you to make local arrangements with the relevant HMCTS legal staff. In these cases you will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. You should also provide the court with a copy of the signed judicial application/order form the next working day.

- 35.6 In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).
- 35.7 Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is your responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

### **Attending a Hearing**

- 35.8 The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.
- 35.9 The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.
- 35.10 You will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. It is envisaged that the case investigator will be able to fulfil this role. The investigator will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. You may consider it appropriate for the SPoC (single point of contact) to attend for applications for CD RIPA authorisations or notices. This does not, however, remove or reduce in any way the duty of you as the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered and which are provided to the JP to make the case.
- 35.11 All application for judicial approval should be referred to Legal services who will advise on who should be presenting RIPA cases to JPs under section 223 of the Local Government Act 1972.

### **Decision**

- 35.12 The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.
- 35.13 **The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.** The JP may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.
- 35.14 If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refused you will need to consider whether they can reapply, for example, if there was information to support the application which was available to you, but not included in the papers provided at the hearing.

35.15 The JP will record his/her decision on the order section of the judicial application/order form. HMCTS administration will retain a copy of the local authority RIPA authorisation or notice and the judicial application/order form. This information will be retained securely.

35.16 The local authority will need to provide a copy of the order to the communications the SPoC (Single Point of Contact) for all CD requests. SPoCs must not acquire the CD requested, either via the CSP or automated systems until the JP has signed the order approving the grant.

## **Outcomes**

35.17 Following their consideration of the case the JP will complete the order section of the judicial application/order form (see form at Annex B) recording their decision. The various outcomes are detailed below:

35.18 The JP may decide to:

- **Approve the Grant or renewal of an authorisation or notice**  
The grant or renewal of the RIPA authorisation or notice will then take effect and you may proceed to use the technique in that particular case.  
In relation to CD, you will be responsible for providing a copy of the order to the SPoC.
- **Refuse to approve the grant or renewal of an authorisation or notice**  
The RIPA authorisation or notice will not take effect and you may not use the technique in that case. Where an application has been refused you may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without you going through the internal authorisation process again. You may then wish to reapply for judicial approval once those steps have been taken.
- **Refuse to approve the grant or renewal and quash the authorisation or notice**  
This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.  
The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

## **Complaints/Judicial Review**

35.19 There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee.

35.20 A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the local authority should consult their legal advisers.

35.21 The IPT will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.

## **36. What do I do with the completed forms?**

36.1 You must send the completed application form(s) to the RIPA Co-ordinating Officer as soon as you are able. This includes any forms in which you have refused authorisation. You should retain a copy of the form and send a further copy to the relevant Investigating Officer for retention on the investigation file. The investigation officer should be advised that it is their

responsibility to ensure that those undertaking the surveillance read the authorization to understand exactly what has been authorised.

## **Monitoring**

### **37. How long will an authorisation last for?**

- 37.1 The authorisation for **Directed Surveillance** will last for **three months** from the date of authorisation unless renewed.
- 37.2 The authorisation for use of a **CHIS** will last for **12 months** from the date of authorisation unless renewed.
- 37.3 It is important to set a review date which gives the opportunity to cancel if the authorisation is no longer required. If the surveillance is still required, set another review date (see below)

### **38. I have now given the authority for surveillance, what should I do next?**

- 38.1 After authorisation the Authorising Officer is responsible for continuing to oversee the progress of the investigation. You must ensure that whatever was authorised does actually happen, and that actions do not exceed the boundaries of the authorisation.
- 38.2 Progress of the investigation or operation should be reviewed in accordance with the review dates set by the authorisation using the relevant review form. In any case, as soon as the investigation or operation objectives have been achieved the authority should be cancelled.
- 38.3 You will regularly monitor the surveillance to ensure:
- Surveillance is being carried out in accordance with the authority given
  - There is still a need for the approved surveillance or use of the CHIS
  - The surveillance is achieving the intended results
  - The risks of collateral intrusion are still minimal
  - The risks associated with the surveillance or use of the CHIS are within an acceptable level
  - The security and/or welfare of the CHIS has not been jeopardised. You must consider any concerns raised by the Investigating Officer relating to the personal circumstances of the CHIS.
- 38.4 You should record the outcome of such monitoring and take whatever action is appropriate.

## **Renewals**

### **39. Why are renewals important?**

- 39.1 Surveillance must cease unless a renewal has been applied for and approved.

**NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.**

### **40. What are my responsibilities in respect of renewals?**

- 40.1 You may renew an authorisation if it is necessary for the authorisation to continue for the purpose for which it was given.

40.2 You must consider the application for renewal in relation to the original purpose for which authorisation was granted, taking into account any change in circumstances. You should be satisfied that:

- There is a need to renew the authorisation (applying the test of necessity)
- That such a renewal is likely to contribute to the investigation or operation (it is proportionate to the aim)
- That the information could not be reasonably obtained by other less intrusive means.
- The risk of collateral intrusion is minimal – you should consider what collateral intrusion has occurred
- The risks associated with the use of a CHIS have not increased beyond an acceptable level

40.3 The outcome of a consideration for renewal may lead to:

- Approval
- A new application
- Refusal

### **Approval**

40.4 If you decide to approve a renewal you will need to provide details of why in your opinion you believe the renewal is justified, and state the date and time when the renewed authorisation will commence and expire on the application form.

40.5 The maximum time that renewal of authorisation can be approved for, is three months at a time for directed surveillance and 12 months for the use of a CHIS, but you may consider shorter periods if this is more appropriate to the circumstances.

40.6 You should also set Review Dates and continue to monitor the progress of the investigation or operation.

### **A new application for authorisation**

40.7 Minor amendments can be made by way of review. However, if significant changes are required e.g. if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then the outstanding authorisation should be cancelled and new authorisation sought by way of a new application. You will need to note the refusal to renew the application on the renewal form setting out the reasons for your decision. You will also need to follow the procedures for cancellation see below and advise the Investigating Officer to seek new authorisation.

### **Refusal**

40.8 If in your opinion surveillance is no longer required, or justified, or proportionate, the renewal should be refused and the authorisation cancelled. See the paragraph on cancellation below. You will need to note on the renewal form your reasons for refusal.

## **41. What do I do with the completed form?**

41.9 You must send the completed renewal form to the RIPA Co-ordinating Officer as soon as you are able. This includes forms where you have refused a renewal. You should retain a copy of the form and send a further copy to the relevant Investigating Officer for retention on the investigation file.

### **Cancellations**



## **42. Why are cancellations important?**

42.1 All authorisations, including renewals, must be cancelled if the reason why directed surveillance or use of a CHIS was required no longer exists or is no longer proportionate. This will occur in most instances when the purpose for which surveillance was required has been achieved and officers must be mindful of the need to cancel any authorisation which has been issued. A cancellation should be issued at the expiry date if not before.

## **43. What are my responsibilities in respect of cancellations?**

43.1 The responsibility to ensure that authorisations are cancelled rests with the Authorising Officer. If you think cancellation should have been applied for, then you should make enquiries of the Investigating Officer as part of your monitoring of the authorisation. On receipt of the cancellation form from the Investigating Officer, you must consider the reasons for cancellation and if acceptable endorse the form.

43.2 As soon as the decision is taken that directed surveillance or use of a CHIS should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject. When cancelling an authorization, an Authorising Officer should:

- record the dates and times (if at all) that surveillance took place and the order to cease the activity was made
- the reason for cancellation
- ensure that surveillance equipment has been removed and returned
- provide directions for the management of the outcomes
- ensure that detail of property interfered with, or person subjected to surveillance, since the last review or renewal are properly recorded
- record the value of surveillance (i.e. whether the objectives as set in the authorization were met

43.3 Where necessary the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled.

## **44. What do I do with the completed form?**

44.1 You must send the completed renewal form to the RIPA Co-ordinating Officer as soon as you are able. This includes forms where you have refused a renewal. You should retain a copy of the form and send a further copy to the relevant Investigating Officer for retention on the investigation file.

## **Working with or through other Agencies**

### **45. What do I do if I want to instruct another organisation to carry out surveillance?**

- 45.1 When some other agency has been instructed on behalf of the Council to undertake some action under RIPA, this Document and the forms in it, must be used in the normal way and the agency advised as necessary of the various requirements. They must be made aware explicitly what they are authorised to do.

### **46. What do I do if I want to carry out an investigation with another organisation?**

- 46.1 It is possible for two public authorities to carry out a joint directed surveillance investigation or use of a CHIS. It must be decided which of the authorities is to take the lead role. The Authorising Officer from the lead organisation must make the decisions on the necessity and proportionality of the surveillance or use of a CHIS. The Investigating Officer must make it clear on the application form that it is a joint investigation and provide details of Officers involved from both authorities.
- 46.2 Where joint surveillance is authorised by the lead organisation, it is good practice for the Investigation Officer of the other organisation to advise their Authorising Officer of the surveillance activity. It is important for each organisation's Authorising Officer to be aware of all surveillance activity being undertaken by their own Investigating Officers, regardless of which organisation authorised the activity.

## **Record-Keeping**

### **47. What records must I keep?**

- 47.1 The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all these forms will be maintained and monitored by the RIPA Co-ordinating Officer.
- 47.2 In all cases, the relevant department should maintain the following documentation:
- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
  - The Magistrates' Order
  - a record of the period over which the surveillance has taken place;
  - the frequency of reviews prescribed by the Authorising Officer;
  - a record of the result of each review of the authorisation;
  - a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
  - the date and time when any instruction was given by the Authorising Officer.
  - a record of the use made of any CHIS

### **48. How long must I keep these records?**

- 48.1 The Council will retain records in accordance with the Council's Record Management Policy. Retention of a record will therefore depend on an assessment of the need to retain the record.

### **49. How should the records relating to a CHIS be maintained?**

- 49.1 Records kept relating to an investigation or operation using a CHIS should be maintained in such a way as to preserve the confidentiality of the CHIS and the information provided by the CHIS.

## **Material obtained from Directed Surveillance and/or use of a CHIS operations**

### **50. How should material be handled and stored?**

- 50.1 Material, or product, such as: written records (including notebook records); video and audio tape; photographs and negatives; and electronic files, obtained under authorisation for Directed Surveillance or use of a CHIS investigations or operations should be handled, stored and disseminated according to the following guidance.
- 50.2 Where material obtained during the course of an investigation may be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with the established disclosure requirements having regard to the Criminal Procedure and Investigations Act 1996 and Civil Procedure Rules.
- 50.3 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 assessed for retention or destruction under the Council's Record Management Policy.

### **51. What about confidential material?**

- 51.1 This is privileged information from, for example, lawyers, doctors, priests etc. Where such persons are involved, and there is a possibility that you maybe obtaining confidential material, then further additional precautions must be taken. If this is the case, please seek appropriate advice from the Monitoring Officer or from the statutory RIPA Code of Practice.

## **Complaints**

### **52. Is there a complaints procedure in place?**

- 52.1 The Regulation of Investigatory Powers Act has established an Independent Tribunal. This Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any cases within its jurisdiction. It also has the power to award compensation.
- 52.2 Details of the relevant complaints procedure can be obtained from the following address:  
  
Investigatory Powers Tribunal  
PO Box 33220  
London  
SW1H 9ZQ
- 52.3 Other actions that could be taken against the Council for failing to meet the requirements of RIPA are civil proceedings under the Human Rights Act 1998 or a complaint to the Ombudsman.

## **Annex A**

### **Senior Responsible Officer (SRO)**

The following Officer shall be designated Senior Responsible Officer on behalf of the Councils under the Codes of Practice:

Simon Copper (Head of Legal and Democratic Services & Monitoring Officer)

### **Authorising Officers (AO)**

The following Officers shall be designated Authorising Officers on behalf of Exeter City Council under the Regulation of Investigatory Powers Act 2000:

Matthew Hall (Team Lead – ECL, Contracts and Licensing)

Danny Damarell (Team Lead – Housing and Litigation)

NB. Only the Chief Executive has the authority to grant authorisation for the acquisition of confidential information or where the authorisation would involve juvenile or vulnerable CHIS

### **RIPA Co-ordinating Officer**

## Annex B

### **Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.**

Local authority:

Local authority department:

Offence under investigation:

Address of premises or identity of subject:

Covert technique requested: (tick one and specify details)

**Communications Data**

☐

**Covert Human Intelligence Source**

☐

**Directed Surveillance**

☐

Summary of details:

**Note:** this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:

Authorising Officer/Designated Person:

Officer(s) appearing before JP:

Address of applicant department:

Contact telephone number:

Contact email address (optional):

Local authority reference:

Number of pages:

**Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.**

Magistrates' court:

Having considered the application, I (tick one):

- ☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- ☐ refuse to approve the grant or renewal of the authorisation/notice.
- ☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes:

Reasons:

Signed:

Date:

Time:

Full name:

Address of magistrates' court: