PROCEDURE FOR ENSURING COMPLIANCE WITH RIPA

(Regulation of Investigatory Powers Act 2000)

Covert Surveillance and Use of Covert Human Intelligence Sources

Revised April 2024
Reviewed April 2024

1.0 OVERVIEW

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") imposes various provisions relating to the interception of communications, acquisition and disclosure of data relating to communications, carrying out of surveillance, the use of covert human intelligence sources and the acquisition of various electronic data. The overall aim is to ensure that such operations are undertaken in accordance with the law and are less vulnerable to challenge under the Human Rights Act 1998.

1.2 This procedure provides guidelines to be followed by officers in relation to undertaking directed covert surveillance and the use of covert human intelligence sources[1] (hereinafter collectively referred to as "surveillance operation"). It does not address any other aspects of RIPA.

1.3 The procedure restricts any surveillance operation that can be undertaken by an officer, and imposes the need for formal authorisations to be secured before any are undertaken. There is also a statutory requirement for authorisations to be approved by the Magistrates' Court.

1.4 Adherence to the provisions of RIPA is monitored by the Investigatory Powers Commissioners Office. Officers should ensure compliance with this procedure at all times, whether or not it is intended to use any information that might be secured from a surveillance operation as evidence in court or other proceedings.

1.5 The Act gives power for codes of practice to be prepared by the appropriate Secretary of State in relation to any surveillance operation. Officers must have regard to any such codes that are for the time being in force in the exercise of a surveillance operation and also be aware that the Codes are revised from time to time. Copies of the codes of practice can be obtained from the Home Office website or from the Monitoring Officer[2].

2.0 DEFINITIONS

2.1 For the purposes of this procedure, the following terms have the definitions identified.

2.2 Collateral Intrusion means the risk of interference with, or intrusion into, the privacy of any person other than those who are the subject of the proposed surveillance operation.

2.3 *Confidential Material* relates to:

2.3.1 matters subject to legal privilege;

2.3.2 confidential personal information relating to a person's physical or mental health, spiritual counselling or other assistance being given or oral or written information arising in the

[1] See paragraphs 2.5 and 2.7 below for meanings

[2] The codes of practice can be obtained on https://www.gov.uk/government/collections/ripa-codes

course of any trade, business etc, that is held subject to an undertaking of confidence or a restriction on disclosure or obligation of secrecy contained in legislation; or

2.3.3 confidential journalistic material being various material acquired or created for the purposes of journalism.

2.4 *Council* means the North Devon District Council.

2.5 *Covert Human Intelligence Source* ("CHIS") means a person who:

2.5.1 establishes or maintains a personal or other relationship with a person for the purpose of facilitating or doing anything within paragraphs 2.5.2 or 2.5.3 below;

2.5.2 uses such a relationship to obtain information or to provide access to any information to another person; or

2.5.3 discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship; and

2.5.4 all in a manner that is calculated to ensure that one of the parties to the relationship is unaware of what is being undertaken.

2.6 *Covert Surveillance* means surveillance that is carried out in a manner calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

2.7 *Directed Covert Surveillance* means covert surveillance that is undertaken for the purposes of a specific investigation or operation, in a manner likely to result in obtaining private information about a person (whether the subject of an investigation or not), otherwise than by way of immediate response to circumstances the nature of which means it would not be reasonably practicable to secure an authorisation for a surveillance operation.

2.8 *Intrusive Covert Surveillance* is covert surveillance that:

2.8.1 is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

2.8.2 involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device (provided that is the case of the use of a surveillance device, surveillance will not be intrusive if the surveillance device is not present on the premises or in the vehicle unless it is a surveillance device that consistently provides information of the same quality and detail as might be expected to be obtained from a surveillance device actually present on the premises or in the vehicle).

2.9 *Necessity* is embracing a requirement to consider why it is necessary to use covert surveillance in the operation as well as establishing the statutory requirement that it must be for the prevention or detection of crime or the prevention of disorder. In respect of directed covert surveillance, there is a also a requirement that the crime must be punishable by at least 6 months imprisonment.

2.10 *Officer* means an individual employed by the council.

2.11 *Proportionality* means requiring the following to be considered:

2.11.1 balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence,
2.11.2 explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others,
2.11.3 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, and
2.11.4 evidencing, as far as reasonably practicable , what other methods had been considered and why they were not implemented.

2.12 *Surveillance* includes:

2.12.1 monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

2.12.2 recording anything monitored, observed or listened to in the course of surveillance; and

2.12.3 surveillance by or with the assistance of any surveillance device.

2.13 *Surveillance Device* means any apparatus designed or adapted for use in surveillance.

3.0 ACTIVITIES SUBJECT TO RIPA

3.1 The following activities that are undertaken by the council are subject to RIPA, and therefore require relevant authorisation:

3.1.1 **Use of Directed Covert Surveillance**
In simple terms, the surveillance of an individual with a view to obtaining private information without their knowledge. This could be through traditional methods of manual observation or through newer more technological focussed methods such as drones, CCTV, ANPR and internet searches.

3.1.2 **Use of a CHIS**
In simple terms, using an individual to interact with another person with a view to obtain information about them without the person knowing. The CHIS may be an officer or a third party. RIPA will still apply.

3.2 Although covered by RIPA, the council does **NOT** have the power to authorise the following activities. **They should not therefore be undertaken**.

3.2.1 Intrusive covert surveillance; and

3.2.2 directed covert surveillance that falls outside the activities for which authorisation may be given.

3.3 A surveillance operation may only be authorised for the purposes of preventing and detecting crime or preventing disorder. An operation consisting of Directed Covert Surveillance is also subject to other restrictions referred to in paragraph 7.1.2.3 later.

4.0 ACTIVITIES UNAFFECTED BY THE ACT

4.1 RIPA does not apply to surveillance that is not covert e.g. the use of overt CCTV surveillance systems for general surveillance (however these are subject to other controls e.g. Data Protection legislation). Guidance on the use of such systems is contained in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012

4.2 General observation undertaken by an officer in the normal performance of his/her duties which does involve the systematic surveillance of an individual will not usually be regulated by RIPA.

4.3 Of relevance to the Council is the fact that covert recording of suspected noise nuisance is unlikely to require an authorisation where the recording is of decibels only or constitutes non-verbal noise such as music or machinery, or if it is the recoding of verbal noise the recording is made at a level which does not exceed that which can be heard with the naked ear from outside the property.

4.4 Surveillance that is undertaken in a manner such that the persons who are subject to the surveillance are aware that it is or may be taking place is not covert. The relevant Codes of Practice provide practicable examples of this.

5.0 THE NEED FOR AUTHORISATION AND SOCIAL MEDIA

5.1 Whenever there is an intention to undertake directed covert surveillance or use a CHIS then an appropriate authorisation **MUST** first be obtained. This can not be avoided by using other individuals or non-governmental organisations to perform the surveillance. In those circumstances, the other organisation is deemed to be an agent of the Council and an authorisation will be required.

5.2 The granting of an authorisation does not allow the investigating officer to ignore normal health and safety requirements. A risk assessment must be conducted before seeking an authorisation and must be available to the Authorising Officer if requested.

SOCIAL MEDIA

5.3 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.'

5.4 If an investigating officer is accessing information on a website or social media site as part of an investigation or operation, the officer will need to consider the intended purpose and scope of the activity that is proposed to be undertaken. The following factors will need to be taken into account in order to decide whether a directed surveillance authorisation is required.

5.4.1 Whether the investigation or research is directed towards an individual or organisation,

5.4.2 Whether it is likely to result in obtaining private information about a person or group of people,

5.4.3 Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile,

5.4.4 Whether information will be recorded and retained,

5.4.5 Whether the information is likely to provide an observer with a pattern of lifestyle,

5.4.6 Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life,

5.4.7 Whether the investigation or research is part of an ongoing piece of work involving repeated viewings of the subject, and

5.4.8 Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject, or information posted by third parties, that may include private information and therefore constitution collateral intrusion into the privacy of these third parties.

5.5 If the investigating officer engages with the individual subject through social media then that individual could become a CHIS requiring management.

5.6 Because of the above and because the scope for obtaining an authorisation to carry out directed covert surveillance or a CHIS is now very limited, the Council's policy is that only the public pages of social media sites should be accessed and then only on a very occasional basis after consideration of the above issues.

5.7 Further guidance on this issue can be found in the Code of Practice.

6.0 WHO CAN GRANT AN AUTHORISATION?

6.1 Authorisation can only be granted by an Authorising Officer who is an officer duly **designated** with the appropriate authority (see also paragraph 10.1).

6.2 Subject to 6.3-6.4 below, the Authorising Officers are those maintained in a list kept by the Monitoring Officer and set out in Appendix 9 of this document.

6.3 Where the use of directed covert surveillance or the use of a CHIS is likely to obtain confidential information or involves the deployment of a juvenile or vulnerable person, authorisation must only be obtained from the Chief Executive or in their absence, the senior officer acting as Chief Executive for these purposes.

6.4 Irrespective of their **designated** power, an officer who is undertaking an investigation should not give authority to him/herself in relation to an investigation/operation in which he/she is directly involved.

6.5 At all times, more senior officers to the investigating officer must authorise the surveillance operation.

7. COVERT SURVEILLANCE

7.1 Applying for Authorisation

7.1.1 An application for authorisation should be made in writing and prepared in a fair and balanced way. A form for this purpose is attached as Appendix 1 [3].

7.1.2 All relevant parts of the application form must be completed by the officer requiring authorisation. In particular, the information provided should:

7.1.2.1 explain in detail the action to be authorised, including any premises or vehicles involved;

7.1.2.2 identify, where known, the subject of the surveillance operation;

7.1.2.3 specify the grounds on which authorisation is sought. An authorisation for directed covert surveillance may only be sought and granted for the purposes of preventing or detecting crime or preventing disorder if it involves a criminal offence that carries a maximum sentence of at least 6 months imprisonment. This means that lesser offences such as dog fouling and fly posting can not be the subject of an application for authorisation. The application must specify which offence is involved and the level of penalty;

7.1.2.4 explain why the surveillance operation is necessary [4];

7.1.2.5 explain why the surveillance operation is considered proportionate. [5] (The issue of proportionality is a concept arising from Human Rights. It applies to both the undertaking of a surveillance operation and the length of time for which it continues. In essence it requires balancing the intrusiveness of the activity on the person the subject of the surveillance operation and any others who might be affected by it against the need for the surveillance in investigative and operational terms. A surveillance operation will not be proportionate if, for example, it is excessive in the overall circumstances, or where the information sought could be obtained using less intrusive methods. Proportionality therefore also necessitates consideration being given towards minimising the scope of the surveillance operation to that which is strictly necessary to achieve the grounds for which it is being undertaken e.g. suspected theft from the workplace may merit surveillance at work, but not at the person's home). The fact that a serious offence is involved will not by itself mean that a surveillance is proportionate. Paragraph 2.11 above sets out the issues that must be considered and explained within the application;

7.1.2.6 identify what information is desired as a result of the authorisation;

---

[3] Appendix 1 contains the form for use when seeking authority for Directed Covert Surveillance. However always refer to the Home Office web-site for the most up to date form – see note 2.

[4] See paragraph 2.9 above.

[5] See paragraph 2.11 above.

7.1.2.7 specifically address the likelihood and extent of intrusion or interference with the privacy of persons other than the subject of the surveillance operation;

7.1.2.8 assess the likelihood of acquiring any confidential material; and

7.1.2.9 identify any surveillance device that is proposed to be used.

7.2 Granting an Authorisation

7.2.1 An officer from whom an authorisation is sought, must have regard to all the information contained in the application form before deciding whether an authorisation should be given.

7.2.2 In particular, the authorising officer should have regard to the following matters before giving authorisation for a surveillance operation:

7.2.2.1 is the activity lawful? All council activities have a statutory basis, and a surveillance operation should not be undertaken unless it is in performance of such an activity e.g. the Environmental Protection Act 1990 (as amended) places a legal duty on the Council to investigate statutory nuisances;

7.2.2.2 is the surveillance operation proportionate [6]?

7.2.2.3 Is the surveillance operation necessary on the ground(s) identified?

7.2.2.4 What is the risk of collateral intrusion? Such an assessment is particularly relevant when considering proportionality, and extra care is necessary in any case where there is special sensitivity (e.g. where the surveillance operation would involve premises used by lawyers or professional counselling, or would occur in any place where the subject of surveillance might expect a high degree of privacy such as his / her home). Whenever practicable, measures should be taken to avoid unnecessary intrusion into the lives of those not directly associated with the surveillance operation.

7.2.2.5 what is the likelihood that confidential material will be obtained? Where it is identified that confidential material may be obtained then, authority for a surveillance operation and the possible obtaining of confidential material **must** only be given by the Chief Executive or in his absence an authorised senior officer acting as Chief Executive for that purpose (but NOT the Monitoring Officer). The authority relating to confidential material must be separately signed in addition to, and at the same time as, a general authority for undertaking the surveillance operation;

7.2.2.6 is the use of any surveillance device acceptable?

7.2.2.7 will the surveillance operation only involve suitably qualified or experienced officers, and if not will any other persons be suitably supervised?

[6] See paragraph 2.11 and 7.1.2.5 above.

7.2.3 Only once the authorising officer has considered all the relevant issues and is satisfied that a surveillance operation ought to proceed should authorisation be granted. Every authorisation must be in writing.

7.2.4 When giving an authorisation, an authorising officer should also identify a time within which the authorisation should be reviewed. In cases involving potential access to confidential information, collateral intrusion or use of vulnerable individuals or juveniles, then more frequent reviews would normally be appropriate.

7.2.5 All completed application forms with their signed authorisation must be sent to the Monitoring Officer within **4 working days** of the day that the authorisation was given. These must be the original forms NOT photocopies.

7.2.6 All application forms must be written including the authorisations. Any amendments must be signed and dated and amendments must only be made by the requesting officer and the authorising officer. Amendments cannot be made after authorisation and submission to the Monitoring Officer.

7.2.7 Following the grant of an authorisation, application must be made to the Magistrates' Court for a hearing to allow the Court to approve the authorisation. Please contact the Legal Department for arrangements to be made for the hearing.

7.2.8 It will be the normal case that the Investigating Officer will be expected to attend at the hearing to support the application. The Authorising Officer may also be required to attend.

7.2.9 For the avoidance of doubt, no action under the authorisation may be taken until the Magistrates' Court has approved the authorisation.

7.2.10 Following the hearing in the Magistrates' Court, the Investigating Officer must provide the Monitoring Officer with the original of any Order issued by the Court within **4 working days** of the hearing, whether the Court approve the authorisation or refuse it.

7.3 Duration and Renewal of Authorisations

7.3.1 Unless renewed an authorisation for directed covert surveillance will cease to have effect after **3 months** from the date that approval is given by the Magistrates Court. An authorisation **must** always be formally cancelled if it is not renewed. It is not acceptable to simply let it expire through the passage of time [7].

7.3.2 Prior to the cessation of any authorisation, the authorising officer can renew an authorisation in writing for a further period of 3 months.

7.3.3 An application for a renewal should normally only be made close to the cessation of the existing authorisation.

7.3.4 A request for a renewal should be submitted to an authorising officer in the appropriate form, copies of which are attached as Appendix 2 [8].

[7] See section 7.4 below for the formal cancelling of operations.
[8] Appendix 2 is for renewals relating to directed covert surveillance.

7.3.5 A request for renewal should in particular contain the following information:

7.3.5.1 whether this is the first renewal or the occasions when the authorisation has previously been renewed;

7.3.5.2 details required for the original authorisation as it applies at the time of the renewal [9];

7.3.5.3 any significant changes to the information;

7.3.5.4 reasons why continued surveillance is necessary;

7.3.5.5 the content and value to the investigation of information so far obtained;

7.3.5.6 whether any privileged material or confidential information was obtained as a result of the activity undertaken under the authorisation,

7.3.5.7 the results of regular reviews of the investigation, and

7.3.5.6 an estimate of the length of time that further surveillance is necessary.

7.3.6 Any authorisation for renewal must be given in writing.

7.3.7 If an authorising officer decides that a renewal should not be granted then reason(s) should be placed on the renewal application and the form amended accordingly to make clear that the renewal has been refused.

7.3.8 Copies of any renewal or of the refusal of renewal must be provided by the authorising officer to the Monitoring Officer within **4 working days** of the day of the renewal being authorised. These must be the original forms NOT photocopies.

7.3.9 In the same way that authorisations must be approved by the Magistrates' Court, applications for renewal must also be approved by the Court. Again, the Legal Department must be consulted in order that a hearing can be arranged. The need to seek approval from the Court must be taken into account when deciding when to apply for a renewal. The application for renewal must be heard by the Court before the authorisation expires.

7.3.10 Once the Court have considered the application for renewal, the original of the Order issued by the Court must be provided to the Monitoring Officer within **4 working days** of the decision, whether the renewal is approved or refused.

7.3.11 Authorisations must be either renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do <u>not</u> lapse with time.**

7.4 Reviews and Cancellations, Record Keeping and Confidential Material

[9] See paragraph 7.1 above.

7.4.1 A review of any extant authorisation shall be undertaken by the authorising officer at such intervals as the authorising officer specifies in the authorisation. Details of the review shall be recorded in writing, appended to the authorisation and a copy provided to the Monitoring Officer within **4 working days** for placing on a central record.

7.4.2 An officer undertaking surveillance or carrying out a review must notify the authorising officer if an investigation unexpectedly interferes with the privacy of individuals not covered by the authorisation. Consideration should at the same time be given as to whether further authorisation is required.

7.4.3 Every authorisation that is granted MUST be formally cancelled. The officer who authorised an investigation, must cancel it if he/she is satisfied that the directed covert surveillance no longer meets the criteria for authorisation. Alternatively an officer can at any time apply in writing for an authorisation to be cancelled. Copies of forms for use in cancellation are attached as Appendix 3 [10].

7.4.4 When an authorising officer decides to cancel a surveillance operation he/she must also make arrangements to ensure that instruction is given to those involved to cease the surveillance operation. The time and date when the instruction is given should be recorded on the cancellation form.

7.4.5 A copy of any cancellation form must be provided by the authorising officer to the Monitoring Officer within **4 working days** for placing on a central record.

Record keeping

7.4.6 Any officer carrying out surveillance should keep a record on a log sheet. A specimen form appears as Appendix 4 [11]:

7.4.6.1 where the log sheet cannot be completed at the time of surveillance, it should be written up as soon as possible thereafter;

7.4.6.2 any alterations in the log sheet should be crossed through with a single line, initialled, and the correct information written to the side. Correction fluid should not be used, and completion of the log should ensure that no empty lines are left where additional information could be written in at a later date;

7.4.6.3 The log sheets might be used in the event of subsequent proceedings and should therefore be signed as true statements, and kept secure at all time.

7.4.7 Any business unit undertaking a surveillance operation should also ensure that once an investigation has been completed all written details associated with it (including the original authorisations, renewals etc) are also kept for at least six years in a secure location and manner where they can be easily found and examined by authorised persons.

[10] Appendix 3 is for use in cancellation of directed surveillance.
[11] Appendix 4 is a specimen log sheet in respect of a Covert Surveillance

Confidential Material

7.4.8 Every officer involved in a surveillance operation should ensure that s/he is familiar with what is meant by confidential material.

7.4.9 If at any time during a surveillance operation an officer is unsure as to whether information that has been obtained may be confidential they should consult with the Legal Services Manager as soon as possible and take steps to ensure that further information is not obtained until the situation is clarified.

7.4.10 The codes of guidance contain specific provisions as to the use of confidential material to which regard must be had at all times.

8. COVERT HUMAN INTELLIGENCE SOURCES

8.1 Applying for Authorisation

8.1.1 An application for authorisation should be made in writing and prepared in a fair and balanced way. Forms for this purpose are attached as Appendix 5 [12].

8.1.2 All relevant parts of the application form should be completed by the officer requiring authorisation. In particular, the information provided should:

8.1.2.1 explain in detail the action to be authorised, including any premises or vehicles involved;

8.1.2.2 identify, where known, the subject of the surveillance operation;

8.1.2.3 specify the grounds on which authorisation is sought. An authorisation for use of a CHIS may only be sought or granted in respect of the prevention or detection of criminal offences or for the prevention of disorder. [13];

8.1.2.4 explain why the surveillance operation is necessary [14];

8.1.2.5 explain why the surveillance operation is considered proportionate [15]. (The issue of proportionality is a concept arising from Human Rights. It applies to both the undertaking of a surveillance operation and the length of time for which it continues. In essence it requires balancing the intrusiveness of the activity on the person the subject of the surveillance operation and any others who might be affected by it against the need for the surveillance in investigative and operational terms. A surveillance operation will not be proportionate if, for example, it is excessive in the overall circumstances, or where the information sought could be obtained using less intrusive methods. Proportionality therefore also necessitates consideration being given towards minimising the scope of the surveillance operation to that which is strictly

[12] Appendix 5 contains the form for use when seeking authority in the case of a CHIS.
[13] See paragraph 3.3 above.
[14] See paragraph 2.9 above.
[15] See paragraph 2.11 above.

necessary to achieve the grounds for which it is being undertaken e.g. suspected theft from the workplace may merit surveillance at work, but not at the person's home). The fact that a serious offence is involved will not by itself mean that a surveillance is proportionate. Paragraph 2.11 above sets out the issues that must be considered and explained within the application;

8.1.2.6 identify what information is desired as a result of the authorisation;

8.1.2.7 specifically address the likelihood and extent of intrusion or interference with the privacy of persons other than the subject of the surveillance operation;

8.1.2.8 assess the likelihood of acquiring any confidential material;

8.1.2.9 identify any surveillance device that is proposed to be used; and

8.1.2.10 identify the persons intended to act as the handler, controller and recorder in respect of the CHIS.

8.1.3 In the case of an application for a CHIS, the information will also include:

8.1.3.1 information relating to the intended CHIS;

8.1.3.2 the purpose for which the CHIS will be used (e.g. in relation to Benefit Fraud);

8.1.3.3 the nature of what the CHIS will be assigned to undertake; and

8.1.3.4 a risk assessment of the activities being undertaken by the CHIS.

8.2 **Granting an Authorisation**

8.2.1 An officer from whom an authorisation is sought, must have regard to all the information contained in the application form before deciding whether an authorisation should be given.

8.2.2 In particular, the authorising officer should have regard to the following matters before giving authorisation for a surveillance operation:

8.2.2.1 is the activity lawful? All council activities have a statutory basis, and a surveillance operation should not be undertaken unless it is in performance of such an activity.

8.2.2.2 is the surveillance operation proportionate [16]?

8.2.2.3 is the surveillance operation necessary on the ground(s) identified N.B. In the case of an investigation where the initial outcome will only result in the service of a notice (e.g. an Abatement Notice or an Enforcement Notice), this will not be an activity for which authorisation can be given [17]?

[16] See paragraphs 2.11 and 8.1.2.5 above.
[17] See paragraph 3.3 for circumstances when a surveillance operation can be authorised.

8.2.2.4 what is the risk of collateral intrusion? Such an assessment is particularly relevant when considering proportionality, and extra care is necessary in any case where there is special sensitivity (e.g. where the surveillance operation would involve premises used by lawyers or professional counselling, or would occur in any place where the subject of surveillance might expect a high degree of privacy such as his / her home). Whenever practicable, measures should be taken to avoid unnecessary intrusion into the lives of those not directly associated with the surveillance operation;

8.2.2.5 what is the likelihood that confidential material will be obtained? Where it is identified that confidential material may be obtained then, authority for a surveillance operation and the possible obtaining of confidential material **must** only be given by the Chief Executive or in his absence an authorised senior officer authorised to act as Chief Executive for these purposes (but NOT the Monitoring Officer). The authority relating to confidential material must be separately signed in addition to, and at the same time as, a general authority for undertaking the surveillance operation;

8.2.2.6 is the use of any surveillance device acceptable?

8.2.2.7 will the surveillance operation only involve suitably qualified or experienced officers, and if not will any other persons be suitably supervised?

8.2.3 In the case of a surveillance operation involving a CHIS, then the following additional issues are also relevant:

8.2.3.1 special consideration should be given to any risk to the CHIS in undertaking the activities proposed;

8.2.3.2 vulnerable individuals (e.g. the mentally impaired) **must** not be used as a CHIS unless the authorising officer of the surveillance operation and the use of the vulnerable individual is the Chief Executive or in his absence a senior officer authorised to act as Chief Executive for these purposes (but NOT the Monitoring Officer). The authority to use the vulnerable individual must be separately signed in addition to, and at the same time as, a general authority for undertaking the surveillance operation;

8.2.3.3 the use of a juvenile as a CHIS (i.e. a person aged under 18 years) requires special consideration, and **under no circumstance** should a CHIS under 16 years of age be authorised to give information against his/her parents [18]. In any event, a juvenile **must** not be used as a CHIS unless the authorising officer of the surveillance operation and use of a juvenile is the Chief Executive or in his absence a senior officer authorised to act as the Chief Executive for these purposes (but NOT the Monitoring Officer). The authority to use a juvenile must be separately signed in addition to, and at the same time as, a general authority for undertaking the surveillance operation.

[18] The codes of guidance identify a number of specific assessments that must be taken before using a juvenile as a CHIS, and reference should be made to them in particular in this respect.

8.2.4 Only once the authorising officer has considered all the relevant issues and is satisfied that a surveillance operation ought to proceed should authorisation be granted. Every authorisation must be in writing.

8.2.5 When giving an authorisation, an authorising officer should also identify a time within which the authorisation should be reviewed. In cases involving potential access to confidential information, collateral intrusion or use of vulnerable individuals or juveniles, then more frequent reviews would normally be appropriate.

8.2.6 All completed application forms with their signed authorisation must be copied to the Monitoring Officer within **4 working days** of the day that the authorisation was given.

8.2.7 All application forms must be hand written including the authorisations. Any amendments must be signed and dated and amendments must only be made by the requesting officer and the authorising officer. Amendments cannot be made after authorisation and submission to the Monitoring Officer.

8.2.8 Following the grant of an authorisation, application must be made to the Magistrates' Court for a hearing to allow the Court to approve the authorisation. Please contact the Legal Department for arrangements to be made for the hearing.

8.2.9 It will be the normal case that the Investigating Officer will be expected to attend at the hearing to support the application and the authorising officer may also be require to attend.

8.2.10 For the avoidance of doubt, no action under the authorisation may be taken until the Magistrates' Court has approved the authorisation.

8.2.11 Following the hearing in the Magistrates' Court, the Investigating Officer must provide the Monitoring Officer with the original of any Order issued by the Court within **4 working days** of the hearing, whether the Court approve the authorisation or refuse it.

8.3 Duration and Renewal of Authorisations

8.3.1 Unless renewed an authorisation for a CHIS will cease to have effect after **12 months** from the day on which approval was provided by the Magistrates Court unless the CHIS is a juvenile in which case it will only last **1 month.** An authorisation must however always be formally cancelled if it is not renewed. It is not acceptable to simple let it expire through the passage of time [19].

8.3.2 Prior to the cessation of any authorisation, the authorising officer can renew an authorisation in writing for a further period of 12 months in the case of a CHIS.

8.3.3 An application for a renewal should normally only be made close to the cessation of the existing authorisation.

[19] See section 8.4 below for the formal cancelling of operations.

8.3.4 A request for a renewal should be submitted to the authorising officer in the appropriate form, copies of which are attached as Appendix 6 [20].

8.3.5 A request for renewal should contain the following information:

8.3.5.1 whether this is the first renewal or the occasions when the authorisation has previously been renewed;

8.3.5.2 details required for the original authorisation as it applies at the time of the renewal [21];

8.3.5.3 any significant changes to the information;

8.3.5.4 reasons why continued surveillance is necessary;

8.3.5.5 the content and value to the investigation of information so far obtained; and

8.3.5.6 an estimate of the length of time that further surveillance is necessary.

8.3.6 Before renewing an authorisation for a CHIS, the authorising Officer must be satisfied that a review has been carried out as to:

8.3.6.1 the use made of the CHIS;

8.3.6.2 the tasks given to the CHIS; and

8.3.6.3 the information obtained from the use or conduct of the CHIS.

8.3.7 Any authorisation for renewal must be given in writing.

8.3.8 If an authorising officer decides that a renewal should not be granted then reason(s) should be placed on the renewal application and the form amended accordingly to make clear that the renewal has been refused.

8.3.9 Copies of any renewal or of the refusal of renewal must be provided by the authorising officer to the Monitoring Officer within **4 working days** of the day that of the renewal being authorised.

8.3.10 In the same way that authorisations must be approved by the Magistrates' Court, applications for renewal must also be approved by the Court. Again, the Legal Department must be consulted in order that a hearing can be arranged. The need to seek approval from the Court must be taken into account when deciding when to apply for a renewal.

[20] Appendix 6 is for renewals involving a CHIS. However, always refer to the Home Office web-site for the most up to date form.

[21] See paragraph 8.1 above.

8.3.11 The application for renewal must be heard by the Court before the authorisation expires. Once the Court have considered the application for renewal, the original of the Order issued by the Court must be provided to the Monitoring Officer within **4 working days** of the decision, whether the renewal is approved or refused.

8.3.12 Authorisations must be either renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do <u>not</u> lapse with time.**

8.4 Reviews and Cancellations

8.4.1 A review of any extant authorisation shall be undertaken by the authorising officer at such intervals as the authorising officer specifies in the authorisation. Details of the review shall be recorded in writing, appended to the authorisation and a copy provided to the Monitoring Officer within **4 working days** for placing on a central record.

8.4.2 An officer undertaking surveillance or carrying out a review must notify the authorising officer if an investigation unexpectedly interferes with the privacy of individuals not covered by the authorisation. Consideration should at the same time be given as to whether further authorisation is required.

8.4.3 Every authorisation that is granted MUST be formally cancelled. The officer who authorised an investigation, must cancel it if he/she is satisfied that the directed covert surveillance no longer meets the criteria for authorisation. Alternatively an officer can at any time apply in writing for an authorisation to be cancelled. Copies of forms for use in cancellation are attached as Appendix 7 [22].

8.4.4 When an authorising officer decides to cancel a surveillance operation he/she must also make arrangements to ensure that instruction is given to those involved to cease the surveillance operation. The time and date when the instruction is given should be recorded on the cancellation form.

8.4.5 A copy of any cancellation form must be provided by the authorising officer to the Monitoring Officer within **4 working days** for placing on a central record.

<u>Record keeping</u>

8.4.6 Any officer carrying out surveillance should keep a record on a log sheet. The requirements of the Regulation of Investigatory Powers (Source Materials) Regulations 2000, or any replacement or amendment, must be complied with. A specimen form appears as Appendix 8 [23]:

8.4.6.1 where the log sheet cannot be completed at the time of surveillance, it should be written up as soon as possible thereafter;

[22] Appendix 7 is for use in cancellation of surveillance involving a CHIS.
[23] Appendix 8 is a specimen log sheet in respect of a CHIS.

8.4.6.2 any alterations in the log sheet should be crossed through with a single line, initialled, and the correct information written to the side. Correction fluid should not be used, and completion of the log should ensure that no empty lines are left where additional information could be written in at a later date;

8.4.6.3 The log sheets might be used in the event of subsequent proceedings and should therefore be signed as true statements, and kept secure at all time.

8.4.7 Any business unit undertaking a surveillance operation should also ensure that once an investigation has been completed all written details associated with it (including the original authorisations, renewals etc) are also kept for at least six years in a secure location and manner where they can be easily found and examined by authorised persons.

Privileged or Confidential Material

8.4.8 Every officer involved in a surveillance operation should ensure that s/he is familiar with what is meant by privileged or confidential material.

8.4.9 If at any time during a surveillance operation an officer is unsure as to whether information that has been obtained may be confidential they should consult with the Legal Services team as soon as possible and take steps to ensure that further information is not obtained until the situation is clarified.

8.4.10 The codes of guidance contain specific provisions as to the use of privileged and confidential material to which regard must be had at all times.

9. ROLE OF MONITORING OFFICER

9.1 The Monitoring Officer shall act as the Senior Responsible Officer under the terms of the Home Office Codes of Practice and is responsible for the general integrity of the processes in place within the Council to manage authorisation. The Monitoring Officer will make arrangements to keep copies of the list of authorised officers, all authorisations and associated documentation provided for a minimum period of three years[24]. The Monitoring Officer will also be responsible for maintaining the central record of authorisations. As part of the record keeping, specific note will be kept of any authorisations relating to confidential material and authorisations for the conduct or use of a vulnerable individual or juvenile as a CHIS. These will be brought to the attention of a relevant inspector when s/he next visits.

[24] The codes of guidance identify the information that must be kept on a central record and made available to the relevant inspector from the Investigatory Powers Commissioners Office.

9.2 The Monitoring Officer shall put in place a system to monitor the expiry and renewal dates of live authorisations and notify authorising officers of impending expiry dates.

9.3 The Monitoring Officer shall undertake an annual review of the operation of this procedure.

9.4 The Monitoring Officer shall ensure that all officers engaged in RIPA activities have received appropriate training for them to carry out their roles efficiently, effectively and lawfully and will be responsible for raising awareness of RIPA issues within the Council.

9.5 The Monitoring Officer can also act as “quality controller” between the application and authorisation procedures.

9.6 The Monitoring Officer will also be responsible for reporting any errors to the Investigatory Powers Commissioner and for putting in place steps to try to ensure errors do not reoccur.

10. ERRORS

10.1 Any relevant errors, which are defined in legislation as being an error in complying with the legislative requirements must be reported to the Monitoring Officer within 2 working days of identification of the error.

10.2 An example of an error would be obtaining an authorisation based on information which is subsequently shown to be incorrect, or the carrying out of surveillance without authorisation.

Appendices 1 – 8
For ease, the necessary Forms have not been reproduced on this copy, but do form part of the policy. They are available on the Home Office website and care should be taken to ensure that only the most up to date forms are used.

APPENDIX 9

List of Officers Able to Grant Authorisations

Ken Miles – Head of Paid Service

Jon Triggs – Head of Resources (Deputy to Head of Paid Service for Confidential authorisations)

Nina Lake – in exercising the Housing and Environmental Health functions held by the Head of Environmental Health and Housing

Monitoring Officer and Senior Responsible Officer

Simon Fuller – Senior Solicitor and Monitoring Officer