



**POLICY AND PROCEDURES
FOR
UNDERTAKING COVERT SURVEILLANCE
AND
USE OF COVERT HUMAN INTELLIGENCE SOURCES**

Regulation of Investigatory Powers Act 2000, as amended.

**THIS DOCUMENT SEEKS TO INCORPORATE CHANGES
MADE AS A RESULT OF THE
PROTECTION OF FREEDOMS ACT 2012 (Ss. 37 & 38)**

**EFFECTIVE AS FROM
1ST NOVEMBER 2012**

RIPA

Contents

PART 1 POLICY FOR UNDERTAKING COVERT SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. Introduction
2. Background
3. New since 1/11 / 2012
4. What is Surveillance?
5. Changes made since 1/11/2012
6. What is a Covert Human Intelligence Source (CHIS)?
7. Procedural principles for Surveillance and use of CHISs

PART 2 PROCEDURE FOR UNDERTAKING DIRECTED SURVEILLANCE

1. Purpose
2. Scope
3. Procedure

PART 3 PROCEDURE FOR USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. Purpose
2. Scope
3. Procedure

Appendices

- Appendix 1. Form: ' Application for Authority for Directed Surveillance'
- Appendix 2. Form: ' Cancellation of Directed Surveillance'
- Appendix 3. Form: ' Review of a Directed Surveillance Authorization'
- Appendix 4. Form: ' Application for Renewal of Directed Surveillance
Authority'
- Appendix 5. Home Office ' Revised Code of Practice – Covert Surveillance'
(printed 8/9/2010).
- Appendix 6. Form: ' Application for Authorization of the Use or Conduct of a
Covert Human Intelligence Source (CHIS)'
- Appendix 7. Form: ' Cancellation of an Authorization of the Use or Conduct of
a Covert Human Intelligence Source (CHIS)'
- Appendix 8. Form: 'Review of a Covert Human Intelligence Source (CHIS)
Authorization'
- Appendix 9. Form: ' Application for Renewal of a Covert Human Intelligence Source
(Chis Application)
- Appendix 10. Annex A- procedure crib sheet.
- Appendix 11. List of Council Authorising Officers
- Appendix 12. Annex B – Judicial Application form
- Appendix 13 . Judicial Approval Order
- Appendix 14. Training powerpoint handout

**& use link to Home Office RIPA website to check
for latest updated Codes of Practice, forms and
information**

Sources of reference are included here but always check for latest sources using the Home Office Link before seeking any authorization and judicial approval

- Home Office Code of Practice – Covert Surveillance (from October 2010)
- Home Office ' Code of Practice – CHIS (from April 2010)
- Home Office Guidance to Local Authorities on the Judicial approval process for Ripa and the Crime Threshold for directed surveillance (October 2012)
- Home Office Guidance for Magistrates' Courts for a Local Authority application seeking an order for approving the grant or renewal of a Ripa authorization or notice (October 2012)
- Summary of Perry v. the United Kingdom
- Home Office Test Purchasing Advice

<http://www.homeoffice.gov.uk/publications/counters-terror/ripa-forms/local-authority-ripa-guidance/?view=Standard&pubID=1079688>

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/>

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/>

PART 1 POLICY FOR UNDERTAKING COVERT SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

1. Introduction

- 1.1 The performance of certain investigatory functions of local authorities may require the surveillance of individuals or the use of informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained, and as such should not be undertaken without full and proper consideration. Legislation now governs how local authorities should administer and record surveillance and the use of informants, and renders evidence obtained lawful for all purposes. This document sets out the Council's policies and procedures for use by all sections of the Council in this respect.
- 1.2 This document is to be used by all Council service areas that undertake investigation work and may use the techniques of surveillance or use of informants. The document is available to members of the public on request.

2. Background

- 2.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force, making it potentially unlawful for a local authority to breach any article of the European Convention on Human Rights (ECHR). Any such breach may now be dealt with by the UK courts directly rather than through the European Court at Strasbourg.
- 2.2 Article 8 of the ECHR states that " Everyone has the right to respect for his private and family life, his home and his correspondence. 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
 - The economic well-being of the country
 - The prevention of disorder or crime
 - The protection of health or morals
 - The protection of the rights and freedoms of others"
- 2.3 The performance of certain functions of local authorities may require the directed covert surveillance of individuals or the use of informants, known as Covert Human Intelligence Sources (CHISs). Those who undertake directed covert surveillance on

behalf of a public authority may breach an individual's human rights unless the covert directed surveillance is pursuant to the exceptions listed in Article 8 of the ECHR, and is both *necessary and proportionate* to the matter being investigated.

- 2.4 In order to properly regulate the use of covert directed surveillance and the use of CHISs in compliance with the HRA, the Regulation of Investigatory Powers Act 2000 (RIPA) came into force on 25th September 2000.
- 2.5 RIPA requires that all applications to undertake covert directed surveillance of individuals or to use CHISs are properly authorized, recorded and monitored. This document sets out the procedures and Codes of Practice for Surveillance and the use of CHISs, and defines and explains the actions that need to be undertaken by officers of the Council prior to undertaking and during such activities, to meet the requirements of RIPA.
- 2.6 Failure to comply with RIPA may leave the Council open to potential claims for damages or infringement of an individual's human rights. It may also mean that any evidence obtained in breach of the provisions of RIPA is rendered inadmissible in Court.

3. NEW SINCE 1ST NOVEMBER 2012

- 3.1 **Ripa has been amended by the Protection of Freedoms Act 2012 so that Local Authority authorizations can only be given effect once a Magistrate has separately approved it by means of a signed Order.**
- 3.2 **The New "crime threshold" applies to the authorisation of directed surveillance by local authorities under RIPA, (but N.B. NOT TO THE AUTHORISATION OF A CHIS.) This came into effect on 1 November 2012.**

4. What is Surveillance?

4.1 Surveillance is:

- Monitoring, observing or listening to persons, their movements, their Conversations or their other activities or communications;
- Recording anything monitored, observed or listened to in the course of Surveillance, with or without the assistance of a device.

- 4.2 By its very nature, surveillance involves invading an individual's right to privacy.

The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy reduces as the individual transfers out into public areas. Within public areas, a relatively low level of privacy can be expected. A judgement in the Strasbourg Court, *Perry v. UK*, clarifies that private life extends to an individual's business and professional activities. A summary of *Perry v. UK* is appended at Appendix 13.

- 4.3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable, and require differing degrees of authorization and monitoring under RIPA.
- 4.4 Authorization is not required for surveillance of the following kinds:
- General observations that do not involve the systematic surveillance of an individual
 - Use of overt CCTV surveillance
 - Surveillance undertaken as an immediate response to a situation
- 4.5 **Overt surveillance** is where the subject of surveillance is aware that it is taking place. Overt surveillance does not contravene the HRA and therefore does not require compliance with RIPA.
For example, the installation of CCTV cameras for the purpose of generally observing activity in a particular area is overt surveillance which does not require authorization.
- 4.6 **Covert surveillance** is defined as "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", and is covered by RIPA. Covert surveillance is categorized as either Intrusive or Directed.
- 4.7 **Intrusive surveillance** is defined as covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle, and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.
- BUT surveillance is not intrusive if:
- It is carried out by a vehicle tracking device
 - It involves the consensual interception of mail or telecommunications for which there is no interception warrant
 - It involves a surveillance device observing residential premises or a private vehicle, which device is not fitted in the premises or vehicle and which device does not consistently provide information of the quality and detail that would be obtained if the device was actually present on the premises or in the vehicle.
 - It involves the use of a television detector for the purpose of detecting a television.
 - **USEFUL information:** See Current Home Office Code of Practice (For link & reference to Co P. & current Orders – see earlier

reference page of this Policy/Procedure document) ie The definition of surveillance as intrusive **relates to the location of the surveillance**, and not any other consideration of the nature of the information that is expected to be obtained. In addition, surveillance under the ambit of the 2010 Order is to be treated as intrusive surveillance. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of *private information*.

RIPA does not empower local authorities to authorize or undertake intrusive surveillance!!

[Following inspection August '09 our Inspector recommended that we specifically note here that "entry on or interference with property or wireless telegraphy also cannot be undertaken by Local Authorities"]

- 4.8 Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:
for the purposes of a specific investigation or operation;
in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically targeted for the purposes of an investigation); and it is carried out otherwise than by immediate response to circumstances when it would not be practical to seek authorization, for example, noticing suspicious behaviour and continuing to observe it.
- 4.9 Private information should be interpreted to include any information relating to an individual's private, family or working life. The concept of private information should be broadly interpreted to include an individual's private, personal or professional relationship with others. Family life should be treated as extending beyond the formal relationships created by marriage. (as explained within the Home Office Code of Practice, see earlier reference page) ***"family" should be treated as extending beyond the formal relationships created by marriage or civil partnership.***
- 4.10 See **Section 26(10) of RIPA**: In relation to a person, includes any information relating to his private or family life.
[The Office of Surveillance Commissioners has advised that It is helpful to have regard to the judgment in the case of **Amann v Switzerland Feb 2000**. In relation to Article 8 it said "...respect for private life comprises the right to establish and develop relationships with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature.]

Surveillance is ***directed*** surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of *private information* about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an *authorisation* under Part II of the 2000 Act to be sought.

Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of *private information*.”

Covert directed surveillance is covered by RIPA and requires prior authorization.

5. CHANGES MADE SINCE 1st November 2012

- 5.1 The Council's Chief Executive and the Executive Management Team endorses this Policy and in particular seeks to ensure that all investigations carried out using the techniques of Ripa fully comply with all statutory provisions.**
- 5.2. The Council's Monitoring Officer ensures that the Council's authorizing officers are of a suitable grade to consider applications and further ensures that both the authorizing officers and investigating officers are appropriately advised and trained.**
- 5.3 The new criminal threshold for directed covert surveillance is applicable. Though we note that this is not the situation for the lawful use of a CHIS.**
- 5.4 The endorsement by means of Judicial approval to give effect to our authorizations provides us with confidence that we act with responsible due diligence in this task.**

6. What is a Covert Human Intelligence Source (CHIS)?

- 6.1 A Council officer or any other person is deemed to be acting as a CHIS if they are attempting to establish a relationship, personal or otherwise, with another person for the purpose of obtaining information about that persons private life, and the purpose of the relationship is not known to that person. **It is not anticipated that CHISs will be used in the normal course of Council investigatory activity.**

If you are considering the use of a CHIS then YOU MUST FIRST CONTACT THE PRINCIPAL LITIGATION SOLICITOR in order that appropriate advice can be given.

- 6.2 Authorization is not required when individuals, including members of the public, are requested to provide information pertaining to other individuals, unless they are required to form a relationship with those other individuals.

7. Procedural principles for Surveillance and use of CHISs

- 7.1 Comprehensive procedures for undertaking directed surveillance and the use of CHISs are given in Parts 2 and 3 of this document.

- 7.2 The conduct of surveillance for these purposes can be undertaken with impunity and with confidence that any evidence obtained will be admissible in a criminal trial provided the conduct is authorized and is carried out in accordance with the authorization. The authorization must be shown to be necessary on the grounds of preventing or detecting crime or of preventing disorder.

- 7.3 The principles of any procedures for surveillance and use of CHISs, in

order to comply with RIPA, are as follows:

- All directed covert surveillance, other than that which is an immediate response to a situation, and all CHIS activity must be authorized at the appropriate level; this should be a senior manager overseeing the service undertaking the investigative activity;
- The Officer requesting authorization for directed covert surveillance or CHIS activity must give very real consideration to the following factors:
 - **Necessity** – is covert surveillance the only or best way to retrieve the desired information, or are there other less invasive methods appropriate, for example overt surveillance; It must also be necessary for the express statutory ground which is available to Local Authorities to undertake covert surveillance
 - **Proportionality** –“*sledgehammer to crack a nut*” - is the surveillance activity proportional to the evidence that will be obtained and

to the privacy the subject could reasonably expect. The methods used to obtain evidence should not be excessive and should be as non-invasive as is possible. The method of surveillance must be proportionate to what is being sought to be achieved.

Sometimes, to demonstrate proportionality it is useful to compare the cost of the proposed surveillance activity with the scope of the problem and to identify how much the activity will impinge on the subjects, eg. How many operatives will be used to carry out the surveillance, for how long, etc etc?

- Collateral intrusion (that is the obtaining of information relating to persons other than the subject of the investigation) and the genuine need to seek to minimise this;
- The risks of the surveillance or CHIS activity must be carefully considered and managed;
- A plan of the operation involving surveillance or CHIS activity should be produced as detailed as possible;
- For CHIS activity, there should be a person with responsibility for recording the use made of the informant;
- All surveillance and CHIS authorizations must be given a unique identification number and a central record kept;
- Judicial approval must be obtained
- **Only once judicial approval has been obtained is an authorization effective**
- Surveillance authorizations remain valid for 3 months, but should be cancelled prior to that if no longer required;
- CHIS authorizations remain valid for one year, but should be cancelled prior to that if no longer required;
- Authorizations should be periodically reviewed by the Authorising Officer and the need for continued surveillance of CHIS activity ascertained; if no longer required authorizations should be cancelled
- If Authorisations need to be renewed, then Judicial approval is required in advance of its expiry
- Urgent authorizations may require seeking judicial approval out of hours.

7.4 Where surveillance or the use of CHISs is likely to result in the obtaining of confidential information, the activity must be authorized by the Chief Executive or in their absence an Executive Director. It is imperative that legal advice is sought prior to activity that may result in confidential information being obtained. Guidance is available in other legislation to show confidential information includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual

counselling concerning an individual (whether living or dead) who can be identified from it. By its very nature, where such information is likely to be acquired, then a higher level of authorization is required than usual.

- 7.5 Services that undertake surveillance activity or use CHISs should put in place adequate arrangements for the retention of evidence gathered. If the evidence is to be used for criminal proceedings the arrangements must comply with current rules of evidence in place from time to time.

Evidence should not be passed to other agencies unless consistent with the original authorization, e.g. passing to the Police for criminal proceedings against offences included on the original authorization.

- 7.6 **Test purchase activity** must be considered carefully and all circumstances concerning the vendor-purchaser activity needs to be considered.

[From 2010 Code of Practice for the use of human intelligence sources para.

2.12:-

“Establishing, maintaining and using a relationship

The word “ establishes” when applied to a relationship means “ set up” . It does not require, as “ maintains” does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity.

Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing he has first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain his trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained."

- 7.7 The Authorising Officer with authority to approve applications for directed surveillance and use of CHISs, subsequent cancellations and renewals is the officer responsible for the management of an investigatory service. The Authorizing Officer's statement on the authorization form should clearly demonstrate agreement that the activity is necessary and proportionate, and that he/she has thoroughly considered the activity before authorizing. A list of current Authorising Officers is approved and maintained by the Council's Monitoring Officer/ Head of Law and is appended at Appendix 11.
- 7.8 The Council's Principal Litigation Lawyer has been assigned the role of the Council's lead officer for RIPA matters. The Principal Litigation Lawyer will maintain the corporate RIPA policy and procedures, ensuring that they reflect the up-to-date legislative situation and that current versions are available to all relevant officers of the Council. The Council's Principal Litigation Lawyer will ensure that arrangements are made for training for Council officers who require it. Additionally the Council's Principal Litigation Lawyer will oversee a programme of refresher training for Authorizing Officers, with the expectation that they will relay key learning points to relevant investigation officers in their teams. The Council's Principal Litigation Lawyer will ensure that any updates to RIPA legislation issued by the Home Office are disseminated promptly to all relevant officers.
- 5.9 The Council's Anti-Fraud & Corruption Team Manager (AFACT) will maintain a central record of authorizations. The central record will be used to track the progress of authorizations and ensure that reviews, renewals and cancellations take place within the prescribed timeframe. Copies of all RIPA authorizations, reviews, renewals and cancellations should be forwarded to the Council's AFACT Manager.

PART 2 PROCEDURE FOR UNDERTAKING DIRECTED SURVEILLANCE

1. Purpose

- 1.1 To ensure that surveillance is only undertaken in appropriate cases, is properly authorized and recorded, and is compliant with the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, as amended by the Protection of Freedoms Act 2012, and appropriate Code of Practices.

2. Scope

- 2.1 This procedure applies to all sections of the Council who routinely or occasionally undertake covert directed surveillance activity.
- 2.2 These procedures apply when the potential surveillance relates to criminal activities.

3. Procedure

- 3.1 All covert directed surveillance activity must be approved prior to the activity taking place. Officers seeking authority to undertake surveillance should complete the form ' Application for Authority for Directed Surveillance' , appended at Appendix 1. Completed application forms should be forwarded to the relevant Authorising Officer, as listed in Appendix 11.
- 3.2 For those matters which are urgent, please first remember that no RIPA authority is required if there is an immediate response to events or situations where it is not reasonably practical to seek prior approval. (see s. 26(2)(c) of RIPA)
- 3.3 In the event that urgent RIPA approval is however necessary then officers and the authorizing officer too will need to ensure that arrangements are made to contact the Magistrates' Court out of hour's service to gain access to a JP.

The telephone number of Bromley Magistrates' Court is 020 8272 105.

- 3.3 It is very important that the correct authorization procedure is followed prior to undertaking surveillance activity. Interference of the right to privacy without proper authorization may render any evidence obtained unusable in a criminal court. If surveillance is conducted on individuals without the necessary authorization, the

Council, and possibly individuals, may be sued for damages for a breach of Human Rights. In civil matters adverse inferences may be drawn from such interference.

- 3.4 All investigating officers and Authorising Officers should fully acquaint themselves with the Code of Practice and refer to it during both the application and authorization processes.
- 3.5 The application for authorization is in two stages 1. Within the Council and if authorized internally then it must be given effect to by 2. Judicial approval being given by means of a signed Order.
- 3.6. THERE IS ONLY ONE GROUND TO SEEK RIPA APPROVAL FOR LAWFUL COVERT DIRECTED SURVEILLANCE :

Local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

THEREFORE, AT THE VERY BEGINNING OF THE INVESTIGATION PROCESS, OFFICERS MUST ENSURE THAT THEY ARE IN FACT INVESTIGATING A CRIMINAL OFFENCE WHICH MEETS THE CRIME THRESHHOLD.

On the Application form for authorization, officers must include **THE ALLEGED OFFENCE** & full details of the reason for the surveillance and the intended outcome of the surveillance. The proposed surveillance activity should be described as fully as possible, with the use of maps or other plans as appropriate. The surveillance activity must be both **necessary** and **proportionate** to the potential offence under consideration and should only be used when other methods of less intrusive investigation have been attempted or are not appropriate. Surveillance authorization forms must include enough detail for the Authorising Officer to make an assessment of proportionality. The application form should include details of the resources to be applied (although tactics and methods should not be included), the anticipated start date and duration of the surveillance, if necessary broken down over stages. Details should also be given of any surveillance previously conducted on the individual. The Authorising Officer must consider these elements, ensuring that the surveillance is **necessary** and **proportionate** before authorising the surveillance

NECESSITY & PROPORTIONALITY:

(Taken from: 2010 CoP: Paras. 3.3 & 3.4 – [Authorising Officers] granting an *authorisation....* for directed ...surveillance,

... must believe that the activities to be authorised are **NECESSARY** on [the] one ... statutory grounds [available to Local Authorities] If the activities are deemed necessary on one of more of the statutory grounds, the person granting the *authorisation* Must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.7 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.8 The following elements of proportionality should therefore be considered:

balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- 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;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.”

3.6 All officers completing RIPA applications, and in particular officers authorizing

- applications, must ensure that applications are sufficiently detailed. Authorizing officers should refuse to authorize applications that are not to the required standard and should refer them back to the originating officers. The Council's Head of Audit & Risk, who maintains the central register of authorizations, will refer forms back to the authorising officer if they fall below the required standard.
- 3.7 The authorization request should detail how officers are going to handle potential collateral intrusion, i.e. those who are unconnected with the subject but who may be affected by the surveillance, and to any information that might be obtained. The application must show what steps are to be taken so as to minimise co-lateral intrusion.
- 3.8 In circumstances where a subject is spotted by chance during other enquiries, they may be followed and observed. This is classified as a direct response to an event and does not require prior authorization.
- 3.9 Local Authorities may NOT conduct intrusive surveillance. It is not permissible to observe an individual in a private dwelling, private vehicle, or in a place where a person would expect a significant level of privacy. If an officer seeks to record the activities of an individual other than in a public place this should be discussed with the relevant Authorising Officer to consider alternative means of investigation.
- 3.10 The Authorising Officer will consider the completed application form. The Authorising Officer will inform the officer making the application of his decision and if it is approved, then the Investigating Officer must seek to give effect to the approval by contacting the local Magistrates' Court.

Applications to the Magistrates' Court:

The Investigating Officer must contact the local Magistrates' Court – Bromley.

Phone them up first : 020 8272 9105. Arrange to attend a hearing with the Authorising officer as well, in their Applications Court to seek Judicial Approval.

The original RIPA authorisation or notice should be shown to the JP but will be retained by the local authority 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). The court may wish to take a copy.

In addition, the local authority will provide the JP with a partially completed judicial application/order form (Annex B).

The Investigating officer will be 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 as this forms the basis of the application for Judicial approval.

The order section of this form will be completed by the JP and will be the official record of the JP's decision.

This procedure, seeking Judicial Approval is necessary for all authorizations/ applications and again for all Renewals!!!

Once Judicial Approval has been given, bring back a copy of the signed Court Order and ensure that a copy of it is provided to the Manager of the Anti-Fraud & Corruption team for it to be kept on the Central Register.

IN RARE MATTERS OF URGENCY:-

If Out of Hours access to a JP is required then it will be for the local authority to make local arrangements with the relevant Court staff. In these cases the local authority will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The local authority should provide the court with a copy of the signed judicial application/order form the next working day.

N.B. There is no requirement for the JP to consider either cancellations or internal reviews.

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.

In addition, that the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

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 the local authority may proceed to use the technique in that particular case.

- **Refuse to approve the grant or renewal of an authorisation or notice**

The RIPA authorisation or notice will not take effect and the local authority may not use the technique in that case.

Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

Once determined at Court:-

The Authorising Officer for the surveillance, must retain a copy of the original authorization form and monitor this for review, renewal and cancellation. The

Authorising Officer is responsible for ensuring that the Head of Audit & Risk is provided with all forms in a timely manner so that a central record can be held.

Each authorization is provided with a Unique number by Head of AFACT giving each authorization a unique identification number using a standard, consistent format. The original authorization should be kept on the investigation file.

- 3.11 The investigating officer and the Authorising Officer must consider the possibility that the surveillance activity may result in the acquiring of confidential information. If this considered to be likely then the investigating officer must state so on the application. The Authorising Officer must then defer the application to the Chief Executive, or in their absence an Executive Director, for consideration and authorization.
- 3.12 The need for Judicial approval will still be required and the procedure is set out above.
- 3.13 Written surveillance authorizations last for a maximum of three months.

So, ensure that you allow sufficient time to seek and obtain that necessary Judicial consent for a Renewal if necessary.

Surveillance authorizations should be cancelled when no longer required. The investigating officer should complete the 'Cancellation of Directed Surveillance' form, appended at Appendix 2, and forward to the relevant Authorising Officer. N.B. When relevant to cancelling authorizations, the Authorising Officer is required to make directions with regard to the "products" of the covert surveillance. See OSC Procedures and Guidance and CoP 2010). All cancellations involving a CHIS must be dealt with following the advice of the Principal Litigation Lawyer.

- 3.14 Each application should be reviewed after an appropriate period of time, and at most one month after the authorization or previous review.. The responsibility for reviewing rests with the Authorising Officer who should conduct the review with the investigating officer. Reviews should not be conducted solely by the investigating officer. Details of the review should be recorded on the form 'Review of a Directed Surveillance Authorization', appended at Appendix 3, and retained with the original authorization. The Authorising Officer must ensure, through diarization or otherwise, that regular reviews are conducted within the correct timeframe.
- 3.15 Applications to renew an authorization can be made by the investigating officer using the form 'Application for Renewal of Directed Surveillance Authority', appended at Appendix 4. Applications for renewal must be made before the expiry of the original authorization. The same conditions for review and cancellation apply to renewals as apply to original authorizations.
- 3.16 Consideration should be given by the investigating officer to notifying the local Police and other relevant agencies in the area of the proposed surveillance activity. This is to ensure that the surveillance activity does not intrude upon or jeopardise

any activity such agencies may themselves be carrying out. The Police or agency should also be notified when the surveillance activity ceases.

- 3.17 The Authorising Officer is responsible for informing the Council's Head of Audit & Risk of all new directed covert surveillance authorizations as soon as such authorization has been given. This is to ensure that an up-to-date central record is maintained for all directed covert surveillance activity. A copy of the authorization form should be forwarded to the Council's Head of Audit & Risk within seven working days, ensuring all details are included. Similarly, all cancellations and renewals should be forwarded to the Council's Head of Audit & Risk using the appropriate forms. The Council's Head of Audit & Risk is responsible for the security of the central record.

PART 3 PROCEDURE FOR USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

Purpose

- 1.1 To ensure that CHIS activity is only undertaken in appropriate cases, is properly authorized and recorded, and is compliant with the Human Rights Act 1998 and Regulation of Investigatory Powers Act 2000 and appropriate Code of Practices, made thereunder.

2. Scope

- 2.1 This procedure applies to all usage of under-cover officers or informants, referred to as Covert Human Intelligence Sources (CHISs). This procedure does not apply to members of the public or Council officers who volunteer information pertaining to other individuals, unless they are required to form a relationship with those other individuals.
- 2.2 This procedure applies to all sections of the Council who routinely or occasionally undertake CHIS activity. (N.B. the new Crime Threshold test pursuant to the Protection of Freedoms Act 2012 does not apply to the use of a CHIS.)
- 2.3 The same considerations apply whether the potential offence or irregularity is criminal or non-criminal. It is anticipated that CHIS activity will be appropriate in predominantly potentially criminal matters. Where investigations concern only civil matters, e.g. tenancy-related investigations, the CHIS activity may still be justified on grounds of the protection of rights of others (e.g. a fraudulent tenancy or illegal sub-let is depriving others on the waiting list of a home).

3. Procedure

- 3.1 All CHIS activity must be approved prior to the activity taking place, except in urgent

circumstances where it is not practicably possible to do so. Officers seeking authority to undertake CHIS activity should complete the form ' Application for Authorization of the Use or Conduct of a Covert Human Intelligence Source (CHIS) ' , appended at Appendix 6. Completed application forms should be forwarded to the relevant Authorising Officer, as listed in Appendix 11.

PLEASE ENSURE THAT IN EVERY CASE THE APPLICANT FOR CHIS AUTHORISATION FIRST CONTACTS THE COUNCIL'S PRINCIPAL LITIGATION LAWYER FOR ADVICE .!!!

- 3.2 It is very important that the correct authorization procedure is followed prior to undertaking CHIS activity. Interference of the right to privacy without proper authorization may render any evidence obtained unusable in a criminal court. If CHIS activity is conducted without the necessary authorization, the Council, and possibly individuals, may be sued for damages for a breach of Human Rights. In civil matters adverse inferences may be drawn from such unlawful interference. This procedure is supported by the Home Office ' Code of Practice

For CHISs, the link to the current Code of Practice is provided using the Home Office Website whose www address is set out on page 4 of this policy and procedures document. All investigating officers and Authorising Officers should fully acquaint themselves with the Code of Practice and refer to it during both the application and authorization processes.

- 3.3 Each CHIS must have a dedicated handler/controller who is responsible for day to day contact with the CHIS. This officer should be identified prior to the authorization being sought.
- 3.3.1 The dedicated handler needs to be an officer, distinct from the Authorising Officer, who is identified to have day-to-day responsibility for dealing with the CHIS on behalf of the Authority, and for the CHIS's security and welfare. The Authorising Officer should maintain oversight of the management of the CHIS. (See the full provisions of s. 29(5) Ripa). See also paragraph 3.11.
- 3.4 The application for authorization must include full details of the reason for the CHIS and the intended outcome of the activity. The necessity for the CHIS activity should be explained. The CHIS activity must be proportionate to the potential offence or irregularity under consideration and should only be used when other methods of less intrusive investigation have been attempted or are not appropriate. CHIS authorization forms must include enough detail for the Authorising Officer to make an assessment of proportionality. The application form must include details of the resources to be applied, the anticipated start date and duration of the activity, if necessary broken down over stages. Details should also be given of any CHIS activity previously conducted on the individual.
- 3.5 The authorization request should be accompanied by a risk assessment, giving details of how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with responsibility for maintaining a record of the use made of the CHIS. The risk assessment should take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become

known. The ongoing security and welfare of the CHIS after the cancellation of the authorization should also be considered at the outset.

- 3.6 The authorization request should detail how officers are going to handle potential collateral intrusion, i.e. those who are unconnected with the subject but who may be affected by the CHIS activity, and to any information that might be obtained. The application must show what steps are to be taken so as to minimise co-lateral intrusion.
- 3.7 The Authorising Officer will consider the completed application form. The Authorising Officer will inform the officer making the application of his decision and if it is approved, will enter details of the CHIS activity into a log held specifically for that purpose.

SINCE 1ST NOVEMBER 2012 JUDICIAL APPROVAL IS REQUIRED TO GIVE EFFECT TO THE CHIS AUTHORISATION AND ANY CHIS RENEWALS.

FULL PRACTICAL DETAILS OF THE JUCIAL APPLICATION AND HEARING PROCEDURE IS SET OUT PREVIOUSLY IN PART 2 FOR DIRECTED SURVEILLANCE – PLEASE REFER.

ONCE JUDICIAL APPROVAL IS PROVIDED:- THEN,

The Authorising Officer will retain a copy of the original authorization form and monitor this for review, renewal and cancellation. & Judicial Approval is required to give effect to every Renewal, not merely the application for authorization. The Head of AFACT is responsible for giving each authorization a unique identification number using a standard, consistent format. The original authorization should be kept on the investigation file.

- 3.7 The need to have a robust system for record keeping is never more apparent than in the context of authorizing the use made of the Chis activity. The Councils Head of AFACT is responsible for maintaining all records relating to the use of the CHIS. The Council' s Principal Housing & Litigation Lawyer will assist the Head of AFACT to ensure full compliance with the statutory provisions in force from time to time.
- 3.8 In urgent circumstances, prior Jucial approvalremains absolutely necessary before effect can be given to lawful use of a CHIS. So, seek advice from the Principal Litigation Lawyer or Head of Law as soon as practical in such circumstances.
- 3.9 The investigating officer and the Authorising Officer must consider the possibility that the CHIS activity may result in the acquiring of confidential information. If this is considered to be likely then the investigating officer must state so on the application. The Authorising Officer must then defer the application to the Chief Executive, or in their absence an Executive Director, for consideration and authorization.
- 3.10 Written CHIS authorizations last for a maximum of 12 months. CHIS authorizations should be cancelled when as no longer required. The investigating officer should complete the ‘ Cancellation of an Authorization of

the Use or Conduct of a Covert Human Intelligence Source (CHIS) form, appended at Appendix 7, and forward to the relevant Authorising Officer. Apart from ensuring that the Authorising Officer makes directions with regard to the management of the product of the covert surveillance (see earlier re: cancellations at Part 2 para 3.12), there is a need to include here ongoing consideration of relevant "welfare" issues arising from the role of CHIS (see approp CoP). Please ensure that all Cancellations concerning CHIS are dealt with following advice from the Council's Principal Litigation Lawyer.

- 3.11 Each CHIS should be managed through a system of tasking and review. Tasking is the assignment given to the CHIS by the handler. (see also paragraph 3.3.1) The task could be asking the CHIS to obtain information, to provide access to information or to otherwise act for the benefit of the Council. The handler is responsible for dealing with the CHIS on a day to day basis, recording the information provided and monitoring the CHIS' s security and welfare. The Authorising Officer should maintain general oversight of these functions.
- 3.12 During CHIS activity there may be occasions when unforeseen action or undertakings occur. Such incidences should be recorded as soon as practicable after the event and, if the existing authorization is insufficient, it should either be updated and re-authorized (for minor amendments only) or it should be cancelled and a new authorization obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new or significantly different way than previously identified, the proposed tasking should be referred to the Authorising Officer, who should consider whether a separate authorization is required. This should be done in advance of any tasking and the details of such referrals must be recorded.
- 3.13 Each application should be regularly reviewed on a monthly basis. The responsibility for reviewing rests with the Authorising Officer who should conduct the review with the investigating officer. Reviews should not be conducted solely by the investigating officer. The review should include a reassessment of the risk assessment, with particular attention given to the safety and welfare of the CHIS. The Authorising Officer should decide whether it is appropriate for the authorization to continue. Details of the review should be recorded on the form ' Review of a Covert Human Intelligence Source (CHIS) Authorization' , appended at Appendix 8, and retained with the original authorization. Cases should be reviewed at no more than one month intervals. The Authorising Officer must ensure, through diarization or otherwise, that regular reviews are conducted within the correct timeframe.
- 3.14 Applications to renew an authorization can be made by the investigating officer using the form ' Application for Renewal of a Covert Human Intelligence Source (CHIS) Authorization' , appended at Appendix 9. Applications for renewal must be made before the expiry of the original authorization. The same conditions for review and cancellation apply to renewals as apply to original authorizations.
- 3.15 Consideration should be given by the investigating officer to notifying the local Police or other relevant agencies in the area of proposed CHIS activity. This is to ensure that the activity does not intrude upon or jeopardize any activity

such agencies may themselves be carrying out. The Police or agency should also be notified when the CHIS activity ceases.

- 3.16 The Authorising Officer is responsible for informing the Council's Head of AFACT of all new CHIS authorizations as soon as authorization and Judicial approval has been given. This is to ensure that an up-to-date central record is maintained for all surveillance activity. A copy of the authorization form should be forwarded to the Council's Head of AFACT within seven working days, ensuring all details are included. Similarly, all cancellations and renewals should be forwarded to the Council's Head of AFACT using the appropriate forms. The Council's Head of AFACT is responsible for the security of the central record.