Appendix A

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

Regulation of Investigatory Powers Act 2000, as amended.

EFFECTIVE AS FROM

1 NOVEMBER 2015 (updated Nov 2016)

RIPA

Contents

Date last Reviewed October 2017

Version No 5

Review date September 2018

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 Authorisation'
Appendix 4.	Form: 'Application for Renewal of Directed Surveillance Authority'
Appendix 5	Home Office 'Revised Code of Practice – Covert Surveillance and Property Interference' (printed 2014).
Appendix 6	Form: 'Application for Authorisation of the Use of a Covert Human Intelligence Source (CHIS)'
Appendix 7	Form: 'Cancellation of an Authorisation of the Use or Conduct of a Covert Human Intelligence Source (CHIS)
Appendix 8	Form: 'Covert Human Intelligence Source (CHIS) Authorisation'
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
Appendix 15	Sources of reference

THIS POLICY, TOGETHER WITH IN-HOUSE TRAINING MATERIALS IS AVAILABLE TO OFFICERS AND MEMBERS.

WHY DO WE HAVE THIS POLICY?

"Local authorities have a wide range of functions and are responsible in law for enforcing over 100 separate Acts of Parliament. In particular local authorities investigate offences in the following areas:

- trading standards, including action against loan sharks, rogue traders, consumer scams, sale of counterfeit goods and unsafe toys and electrical goods; and
- environmental health, including action against large-scale waste dumping, dangerous workplaces, pest control and the sale of unfit food; and

Local authorities are also responsible for tackling issues as diverse as anti-social behaviour, unlicensed gambling, and threats to children in care, underage employment and taxi regulation. As part of their investigation a local authority may consider that it is appropriate to use surveillance to obtain evidence.

Local authorities use three investigatory techniques that can be authorised under RIPA:

- directed surveillance;
- use of a covert human intelligence source; and
- obtaining and disclosing communications data

RIPA does not allow the use of any other covert techniques to be used by local authorities. In particular, a local authority cannot be authorised under RIPA to intercept the content of a communication.

Approval of local authority use of RIPA

From 1 November 2012 local authorities were required to obtain judicial approval prior to using covert techniques. Local authority authorisations and notices under RIPA will only be given effect once an order has been granted by a justice of the peace (JP) in England and Wales, a sheriff in Scotland and a district judge (magistrates' court) in Northern Ireland.

Additionally, from this date local authority use of directed surveillance under RIPA will be limited to the investigation of crimes which attract a 6 month or more custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco." [Home Office Guidance overview printed March 2014]. The Council has a separate policy with regard to 'Non-RIPA surveillance'.

It should be noted that on the 1st September 2017 The Office of Surveillance Commissioners was abolished by the Investigatory Powers Act 2016 and replaced by the Investigatory Powers Commissioners Office (IPCO).

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

1.0 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 bring 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 and enforcement activities and may use surveillance or informants. This document is available to members of the public on request.

2.0 Background

2.1. On 2 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; or
- 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 that is why all such directed surveillance should be 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 authorised, recorded and monitored. This document sets out the Council's policy and procedures for the use of Surveillance and CHISs in accordance with RIPA. It is possible that the Council will undertake surveillance without RIPA authorisation, and has a separate policy in this regard. This policy and procedure 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.

3.0 New since 1 November 2012

3.1 RIPA was amended by the Protection of Freedoms Act 2012 so that local authority authorisations can only be given effect once a Magistrate has separately approved it by means of a signed order.

3.2 The "crime threshold" applies to the authorisation of directed surveillance by local authorities under RIPA, but not to the authorisation of the use of a CHIS.

4.0 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, further clarifies this within the context of privacy for an individual. 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 authorisation and monitoring under RIPA.

4.4 Authorisation 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; or
- 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.

4.6 For example, the installation of CCTV cameras for the purpose of generally observing activity in a particular public area is overt surveillance which does not require authorisation.

4.7 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.

4.8 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. However, 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; or
- It involves the use of a television detector for the purpose of detecting a television

4.9 RIPA does not empower local authorities to authorise or undertake intrusive surveillance.

4.10 The local authority does not have the power to interfere with property or wireless telegraphy or undertake intrusive surveillance operations (i.e. covert surveillance in relation to anything taking place on residential premises or a private vehicle carried out either by a person or device inside residential premises or a private vehicle or by a device placed outside.

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

- for the purposes of a specific investigation or operation; and
- 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 authorisation, for example, noticing suspicious behaviour and continuing to observe it.

4.12 "The Council can use directed surveillance only for the purpose of preventing and detecting conduct which constitutes one or more criminal offences and it meets one of the following conditions:

(a) That the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months imprisonment ; or

(b) Would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. (All offences involving sale of tobacco and alcohol to underage children.)"

[See Article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (as amended) an d s. 55 of the Home Office guidance on the judicial approval process for RIPA and the crime threshold for directed surveillance.]

4.13 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 or civil partnership.

4.14 See Section 26(10) of RIPA: In relation to a person, includes any information relating to his private or family life. The Investigatory Powers Commissioner's Office 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.

4.15 See sections 2.4 - 2.7 of the Home Office Covert Surveillance and Property Interference Code of Practice.

4.16 "Private life considerations are likely to arise if several records are to be analysed together in order to establish a pattern of behaviour, or if one or more pieces of information (whether or not in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In some circumstances, the totality of the information gleaned may constitute private information even if the individual records do not. Where such information is acquired by means

of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate."

4.17 Thus, the planned covert surveillance of a specific person, 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 authorisation.

5.0 CHANGES MADE SINCE 1 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 Authorising Officers are of a suitable grade to consider applications and further ensures that both the Authorising 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 authorisations (including the use of any CHIS) provides us with confidence that we act with responsible due diligence in this task.

6.0 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 establish or maintain a personal or other relationship, with a person for the covert purpose of facilitating the following:

- they covertly use such a relationship to obtain information or to provide access to any information to another person; or
- They covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such 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. [see para 2 CoP 2014)

6.2 Whilst it is not anticipated that CHISs will be used in the normal course of Council investigatory activity in the event that it is thought necessary, it is imperative and indeed a legal requirement that enhanced authorisation arrangements are in place.

6.3 If you are considering the use of a CHIS then you must first contact the Principal Litigation Lawyer in order that appropriate advice can be given.

6.4 Authorisation 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.

6.5 A member of the public may provide information to the Council even though they have not been tasked or requested to do so. It is important to

note that an Informant might be considered a CHIS if the information which s/he passes to the council has been obtained in the course of (or as a consequence of the existence of) a personal or other relationship, even if that relationship was not established for the purpose of obtaining it. In the event of this occurring guidance should be sought from the Principal Lawyer.

7.0 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 authorised and is carried out in accordance with the authorisation. The authorisation 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 authorised at the appropriate level; this should be by a Council Authorising Officer from a service other than the investigating service.
- For the CHIS authorisations, enhanced authorisation is required with the support of the Council's Principal Litigation Lawyer, through the office of the Council's Chief Executive or in his absence an Executive Director.
- The Officer requesting authorisation for directed covert surveillance or CHIS activity must give very real consideration to the following factors (noted here and again later at page 19):
    - Necessity – is covert surveillance the only or best way to retrieve the desired information, or are there other less invasive methods, for example overt surveillance. It must also be necessary for the express statutory duty which the local authorities is undertaking
- Proportionality" - is the surveillance activity proportionate 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 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 subject, e.g. how many operatives will be used to carry out the surveillance, for

how long, 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 authorisations 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 authorisation effective**
- Surveillance authorisations remain valid for 3 months, but should be cancelled prior to that if no longer required;
- CHIS authorisations remain valid for one year, but should be cancelled prior to that if no longer required;
- Authorisations should be periodically reviewed by the Authorising Officer and the need for continued surveillance of CHIS activity ascertained; if no longer required authorisations should be cancelled
- If authorisations need to be renewed, then Judicial approval is required in advance of its expiry
- Urgent authorisations 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 authorised 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 authorisation 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.

7.6 Evidence should not be passed to other agencies unless consistent with the original authorisation, e.g. passing to the Police for criminal

proceedings against offences included on the original authorisation.

7.7 Test purchase activity must be considered carefully and all circumstances concerning the vendor-purchaser activity needs to be considered.[From 2014 Code of Practice for the use of human intelligence sources para. 3.12, 6.7 and 6.14 -6016 in the context of test purchasing]

7.8 Real awareness for care regarding the use of vulnerable adults or juveniles as sources, particularly within the context of test purchasing is needed.

FOR THE PURPOSES OF TEST PURCHASING:-

7.9 If such test purchasing is a one- off, in retail premises accessible to the public, then it is reasonable to assume that:

7.10 Surveillance is unlikely to be conducted in such a way as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation), and

7.11 The test purchase is not a CHIS because he/ she does not establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the obtaining of information.

7.12 For example: routine one- off test purchases including tests for potential breaches of the Licensing Act 2003.

7.13 However, be careful: the advice here would be different if the test purchaser had made previous visits to the premises to gain the trust of the retailer that could be creating a CHIS. Or perhaps if the test purchase had occurred from within someone's home including part of a home adjacent to a retail premises – that could be deemed to be intrusive.

For situations with a CHIS:

7.14 There are special requirements with regard to the management, security and welfare of sources. You are urged to refer to the current Code of Practice for CHIS : in particular:

- When deploying a source, the Council should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, including the foreseeable consequences to others of that tasking
- Before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences, should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

7.15 The person responsible for the day to day management of the source's welfare and security, will bring to the attention of the Authorising Officer, any concerns about the personal circumstances of the source, in so far as they might affect – the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. This may all have a

bearing for the Authorising Officer as to whether or not the authorisation should continue.

7.16 **Example:** 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.

7.17 The appropriate Authorising Officers 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, (and the Chief Executive / Executive Director where relevant.) The Authorising Officer/ Executive Director Authorisation form should clearly demonstrate agreement that the activity is necessary and proportionate, and that he/she has thoroughly considered the activity before authorising. A list of current Authorising Officers is approved and maintained by the Council and can be found at Appendix 11.

7.18 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 Authorising 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.

7.19 The Council's Anti-Fraud & Corruption Team Manager (A-FACT) will maintain a central record of authorisations. The central record will be used to track the progress of authorisations and ensure that reviews, renewals and cancellations take place within the prescribed timeframe. Copies of all RIPA authorisations, reviews, renewals and cancellations should be forwarded to the Council's A-FACT Manager.

7.20 The Council's Chief Executive or one of his Executive Directors ONLY must be the Authorising Officer for the following:

- matters subject to legal privilege,
- confidential constituent information between the Councillor and a constituent in respect of constituency matters,
- Confidential personal information, (e.g. Medical confidential information, or spiritual personal information) or
- Confidential journalistic material (e.g. has been acquired for the purpose of journalism only).

PART 2 PROCEDURE FOR UNDERTAKING DIRECTED SURVEILLANCE

1.0 Purpose

1.1. To ensure that surveillance is only undertaken in appropriate cases, is properly authorised 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.

2.0 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.

3.0 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 authorising 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 phone number of Bromley Magistrates' Court is 020 8437 3585.

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

3.5 All investigating officers and Authorising Officers should fully acquaint themselves with the Code of Practice and refer to it during both the application and authorisation processes.

3.6 The application for authorisation is in two stages 1. Within the Council and if authorised internally then it must be given effect to by 2. Judicial approval being given by means of a signed Order.

3.7 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 THRESHOLD.

3.8 On the Application form for authorisation, officers must include the alleged offence and 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.

3.9 Surveillance authorisation 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.

3.10 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:

3.11 (See sections 3.3 -3.6 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 3.2 – 3.4 Covert Human Intelligence Sources Code of Practice.)

3.12 Proportionality- is a fundamental principle embodied within the HRA. Officers must be able to demonstrate that a covert surveillance operation justifies the level of intrusion of privacy that may occur with regard to the target(s) of the surveillance or any other persons – it must be proportionate when set against the outcome.

3.13 Authorising officers must be assured that the activities to be authorised are necessary in relation to Directed surveillance and for a CHIS where relevant. In addition authorising officer must be assured that the activities 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 target or any other person affected by the covert

surveillance, against the need for the activity, in investigative and operational terms.

3.14 Full reasons why the planned activity is considered proportionate must be adequately recorded in the application form including

- A balance of the size and scope of the planned activity against the gravity and extent of the perceived crime;
- An explanation as to how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- A consideration as to whether the activity is an appropriate and reasonable use of the legislation, having considered all the reasonable alternatives of obtaining the necessary result,
- Evidence of the other methods that have been considered and why they have not been used.

3.15 The Authorising Officer will only grant the application if it is considered by him/ her to be necessary in the circumstances of the particular case.

3.16 Surveillance activity will not be proportionate if it is excessive in the overall circumstances of the cases.

COLLATERAL INTRUSION

3.17 (See sections 3.8 -3.11 and 3.8 -3.11 of the two respective Codes of Practice referred to above)

3.18 The risk of collateral intrusion must be looked at in every application and wherever possible either avoided or minimised. The privacy of other persons must be protected – for example the innocent bystanders. Unnecessary intrusion into the lives of those not directly involved must be addressed by measures to be considered in every case. The investigating officer and Authorising Officer must consider the proportionality of any collateral intrusion and whether sufficient measures are to be taken to limit it.

3.19 The authorisation will <u>not</u> 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.

3.20 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.

3.21 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 alternative methods, of obtaining the necessary result;

- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

3.22 All officers completing RIPA applications, and in particular officers authorising applications, must ensure that applications are sufficiently detailed. Authorising officers should refuse to authorise applications that are not to the required standard and should refer them back to the originating officers. The Council's A-FACT Manager, who maintains the central register of authorisations, will refer forms back to the authorising officer if they fall below the required standard.

3.23 The authorisation request should detail how officers are going to manage potential collateral intrusion i.e. how information gathered in regard to those who are unconnected to the investigation will be dealt with. The application must show what steps are to be taken so as to minimise co-lateral intrusion.

3.24 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 authorisation.

3.25 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.

3.26 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:

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

3.28 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.

3.29 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.

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

3.31 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.

3.32 The order section of this form will be completed by the JP and will be the

official record of the JP's decision.

3.33 This procedure, seeking Judicial Approval is necessary for all authorisations/ applications and again for all Renewals.

3.34 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:-

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

3.36 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.

3.37 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.

3.38 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.

3.39 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.

3.40 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.

3.41 Once determined at Court:

- The Authorising Officer for the surveillance, must retain a copy of the original authorisation form and monitor this for review, renewal and cancellation. The Authorising Officer is responsible for ensuring that the A-FACT Manager is provided with all forms in a timely manner so that a central record can be held.

- Each authorisation is provided with a unique number by the A-FACT Manager giving each authorisation a unique identification number using a standard, consistent format. The original authorisation should be kept on the investigation file.

3.42 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 authorisation.

3.43 The need for judicial approval will still be required and the procedure is set out above.

3.44 Written surveillance authorisations last for a maximum of three months, therefore ensure that you allow sufficient time to seek and obtain that necessary judicial consent for a Renewal if necessary.

3.45 Surveillance authorisations 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 authorisations, the Authorising Officer is required to make directions with regard to the "products" of the covert surveillance. All cancellations involving a CHIS must be dealt with following the advice of the Principal Lawyer.

3.46 Each application should be reviewed after an appropriate period of time, and at most one month after the authorisation 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 Authorisation', appended at Appendix 3, and retained with the original authorisation. The Authorising Officer must ensure, through diarization or otherwise, that regular reviews are conducted within the correct timeframe.

3.47 Applications to renew an authorisation 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 authorisation. The same conditions for review and cancellation apply to renewals as apply to original authorisations.

3.48 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.

3.49 The Authorising Officer is responsible for informing the Council's Head of Audit & Risk of all new directed covert surveillance authorisations as soon as such authorisation 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 authorisation form should be forwarded to the Council's A-FACT Manager within seven working days, ensuring all details are included. Similarly, all cancellations and renewals should be forwarded to the Council's A-FACT Manager using the appropriate forms. The Council's A-FACT Manager is responsible for the security of the central record.

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

1.0 Purpose

1.1. To ensure that CHIS activity is only undertaken in appropriate cases, is properly authorised 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.

2.0 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 use of a CHIS will only be appropriate in matters for the prevention or detection of crime or the prevention of disorder.

3.0 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 Authorisation 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 authorisation procedure is followed prior to undertaking CHIS activity. Interference of the right to privacy without proper authorisation may render any evidence obtained unusable in a criminal court. If CHIS activity is conducted without the necessary authorisation, 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

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

3.4. Each CHIS must have a dedicated handler who is responsible for day to

day contact with the CHIS. This officer should be identified prior to the authorisation being sought.

3.5. 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 CHISs 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.

3.6. The application for authorisation 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 authorisation 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.

3.7. Most important: the authorisation 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 authorisation should also definitely be considered at the outset.

3.8. The authorisation 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 collateral intrusion.

3.9. 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.

JUDICIAL APPROVAL IS REQUIRED TO GIVE EFFECT TO THE CHIS AUTHORISATION AND ANY CHIS RENEWALS. FULL PRACTICAL DETAILS OF THE JUDICIAL APPLICATION AND HEARING PROCEDURE IS SET OUT PREVIOUSLY IN PART 2 FOR DIRECTED SURVEILLANCE – PLEASE REFER.

3.10. The Authorising Officer will retain a copy of the original authorisation form and monitor this for review, renewal and cancellation. A judicial approval is required to give effect to every renewal, not merely the application for authorisation. The A-FACT Manager is responsible for allocating each authorisation a unique identification number using a standard, consistent format. The original authorisation should be kept on the investigation file.

3.11. The need to have a robust system for record keeping is never more apparent than in the context of authorising the use made of the CHIS activity. The Council's A-FACT Manager is responsible for maintaining all records relating to the use of the CHIS. The Council's Principal Litigation Lawyer will assist the Council' A-FACT Manager to ensure full compliance with the statutory provisions in force from time to time.

3.12. In urgent circumstances, prior judicial approval remains 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.

3.13. 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 authorisation.

3.14. Written CHIS authorisations last for a maximum of 12 months. CHIS authorisations should be cancelled when as no longer required. The investigating officer should complete the 'Cancellation of an Authorisation of the Use or Conduct of a Covert Human Intelligence Source (CHIS)' form, appended at Appendix 7, and forwarded 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 appropriate CoP). Please ensure that all Cancellations concerning CHIS are dealt with following advice from the Council's Principal Litigation Lawyer.

3.15. 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.

3.16. 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 authorisation is insufficient, it should either be updated and re-authorised (for minor amendments only) or it should cancelled and a new authorisation 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 authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

3.17. 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 authorisation to continue. Details of the review should be recorded on the form 'Review of a Covert Human Intelligence Source (CHIS) Authorisation', see Appendix 8, and retained with the original authorisation. 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.

3.18. Applications to renew an authorisation can be made by the investigating officer using the form 'Application for Renewal of a Covert Human Intelligence Source (CHIS) Authorisation', appended at Appendix 9. Applications for renewal must be made before the expiry of the original authorisation. The same conditions for review and cancellation apply to renewals as apply to original authorisations.

3.19. 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.

3.20. The Authorising Officer is responsible for informing the Council's A-FACT Manager of all new CHIS authorisations as soon as authorisation 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 authorisation form should be forwarded to the Council's A-FACT Manager within seven working days, ensuring all details are included. Similarly, all cancellations and renewals should be forwarded to the Council's A-FACT Manager using the appropriate forms. The Council's A-FACT Manager is responsible for the security of the central record.

Appendix 15

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

- https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice
- Home Office Code of Practice /publications/covert-sand Property Interference (from December 2014)
- Home Office Code of Practice – Covert Human Intelligence Sources (from December 2014)
- And the Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (Home Office guidance for Magistrates' Courts in England and Wales for a local authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice.
- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf
- 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 authorisation or notice (October 2012)
- Summary of Perry v. the United Kingdom
- Home Office Test Purchasing Advice
- http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/