WESTMINSTER CITY COUNCIL

DIRECTED SURVEILLANCE
COMMUNICATIONS DATA
COVERT HUMAN INTELLIGENCE SOURCES

PROCEDURE MANUAL

PURSUANT TO THE REGULATION OF INVESTIGATORY POWERS ACT 2000

This manual has been prepared to assist officers of the Council to guide them on the use of Directed Surveillance, Communications Data and Covert Human Intelligence Sources. It is not intended to be an exhaustive guide and specific legal advice should be sought if officers do not find their questions answered after reading this manual and the various Codes mentioned in it. Officers can also contact the Authorising Officers listed in the appendix to this manual.

Reviewed - March 2016

CONTENTS

1. Introduction

Background

1.1 Covert Surveillance is regulated by Part II of the Regulation of Investigatory Powers Act 2000 ("RIPA"). The Home Office has issued revised Codes of Practice to provide guidance to public authorities on the use of RIPA to authorise covert surveillance, which is likely to result in the obtaining of private information. The revised Codes of Practice are titled "Covert Surveillance and Property Interference" and "Covert Human Intelligence Sources". The Home Office has also issued guidance on obtaining Judicial Approval of RIPA authorisations from the Magistrates' Court. This guidance is titled, "Home Office Guidance to Local Authorities in England and Wales on the Judicial Approval Process for RIPA and the crime Threshold for Directed Surveillance".

Effect of the Codes of Practice

1.2 All Codes of Practice issued pursuant to section 71 of RIPA are admissible as evidence in criminal and civil proceedings. If any provision of the Codes appear to be relevant to a court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal established under RIPA, or to one of the Commissioners responsible for overseeing the powers conferred by RIPA, they must be taken into account.

1.3 This Procedure Manual sets out the procedures that must be followed when the Council undertakes authorised covert surveillance and brings into effect a number of changes that have been implemented by the revised Codes. The Protection of Freedoms Act 2012 brought in the need to seek Magistrates' approval. Further changes to the conditions for Directed Surveillance were brought in by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 ("the 2012 Order"), which was made on 11 June 2012 and came into force on 1 November 2012.

1.3 It is intended to be a best practice guide. This Manual is not intended to replace the Home Office Codes but following this guidance will ensure compliance with those Codes.

Surveillance activity to which this Manual applies

1.4 RIPA provides for the authorisation of covert surveillance by public authorities where that surveillance is likely to result in the obtaining of private information about a person.

1.5 Surveillance, for the purposes of RIPA, includes monitoring, observing or listening to persons, their movements, conversations or other activities. It may be conducted with or without assistance of a surveillance device and includes the recording of information obtained.

1.6 Surveillance is covert if, and only if, it is carried out in a manner which is calculated to ensure that any person who is the subject of the surveillance is unaware that it is or is likely to be taking place.

1.7 Covert Surveillance as regulated by RIPA falls into two categories:

- directed surveillance; and
- intrusive surveillance.

The Council has the power to authorise its officers in relation to directed covert surveillance and also in relation to Covert Human Intelligence Sources ("CHIS"), although this power is rarely used. However, this manual predominantly deals with this category of covert surveillance. However, reference is made to intrusive covert surveillance to ensure that officers do not unwittingly cross the threshold into this type of surveillance, which would be unlawful.

Basis for lawful surveillance activity

1.8 The Human Rights Act 1998 gave effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). By its very nature, covert surveillance compromises an individual's right to respect for his private and family life, which is a fundamental right under Article 8 of the ECH. However, this is a qualified right, which means that it can be interfered with, provided such interference is justified on certain grounds.

1.9 Article 6 of the ECHR, the right to a fair trial, is also relevant where a prosecution follows the use of covert techniques.

1.10 Evidence that is obtained by the use of covert surveillance may be ruled inadmissible by the courts under section 78 of the Police and Criminal Evidence Act 1984, if it has been obtained unfairly or in a manner which is found to be an abuse of process.

1.11 Therefore, RIPA provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. Failure to comply with the provisions of RIPA may result in the Council being liable to pay compensation for breach of Human Rights or may lead to a complaint being made to the Investigatory Powers Tribunal. This could also attract criticism from the Commissioners on their regular inspections.

1.12 Following the procedures set down in this Manual will limit any challenges that may be bought either for breach of a person's human rights or for inadmissibility of evidence. Compliance with this Manual will also ensure that any complaint to the RIPA Tribunal can be successfully defended as can any complaint that is made to the Local Government Ombudsman.

1.13 Covert Surveillance is likely to involve the processing of personal data or personal information and as such the Data Protection Principles enshrined within the Data Protection Act 1998 must be complied with to ensure that data

is processed fairly and lawfully. This is in addition to having to comply with the requirements of RIPA.

2. When can a Local Authority authorise covert surveillance?

2.1 An authorisation may not be granted under section 28 (directed covert surveillance) unless it meets the following two conditions -

1. that the authorisation is for a purpose of preventing or detecting conduct which –

   (a) constitutes one or more criminal offences, **or**

   (b) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one of more criminal offences; **and**

2. that the criminal offence is or would be –

   (a) an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or

   (b) an offence under –

   (i) section 146 of the Licensing Act 2003 (sale of alcohol to children);or

   (ii) section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children); or

   (iii) section 147A of the Licensing Act 2003 (persistently selling alcohol to children); or

   (iv) section 7 of the Children and Young Persons Act 1933 (sale of tobacco etc., to persons under eighteen)

2.2 The test for a CHIS is contained within section 29(3) of the Act. A CHIS can be authorised for the purpose of preventing or detecting crime and disorder and does not require an offence to be punishable, whether on summary conviction or an indictment, by a maximum level of at least 6 months imprisonment.

3. What is Directed and Intrusive Surveillance?

3.1 **Directed surveillance** is defined in section 26(2) of RIPA as surveillance that is covert but not intrusive and is undertaken:

a) for the purposes of a specific investigation or operation;
b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought for the carrying out of surveillance.

3.2 **Intrusive Surveillance** is defined by section 26(3) of RIPA as covert surveillance that:

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

(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Put simply, any covert surveillance which obtains private information which could only be obtained from within a person's home or motor vehicle, is more than likely intrusive surveillance, and should not be undertaken by the Council at all.

4. What is Private Information?

4.1 RIPA states that private information includes any information relating to a person's private and family life, his home and his correspondence. Private information should be taken generally to include any aspect of a person's private or personal relationships with others, including family and professional or business relationships.

4.2 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is made by a public authority of that person's activities for future consideration.

Example: Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to covertly record or listen to the conversation as part of a specific investigation or operation.

4.3 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or where 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. In such circumstances, the totality of information gleaned may constitute private information even if the individual records do not. Where such conduct includes covert surveillance, then an authorisation for directed surveillance should be sought.

Example: Officers of a local authority wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this

nature is not likely to require directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise to, say, establish a pattern of occupancy of the premises by any person the accumulation of information is likely to result in the obtaining of private information about that person and an authorisation should therefore be considered.

4.4 Private information may also include personal data, such as names, telephone numbers and address details. 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. However, consideration should always be given to whether there are any other lawful and less intrusive means of obtaining personal data.

5. When is authorisation not required?

5.1 Some surveillance activity does not constitute directed surveillance for the purposes of RIPA and therefore no authorisation can be sought or is necessary. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- overt use of CCTV and ANPR systems

Immediate response to events:

5.2 Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events, in such a way that it is not reasonably practicable to obtain authorisation under RIPA, would not require a directed surveillance authorisation to be in place prior to the surveillance being carried out. RIPA is not intended to prevent law enforcement officers fulfilling their legislative functions. However, an Authorisation Form should be completed and filed on the Central Record as soon as practicable after the event.

General observation activity:

5.3 General observation forms a significant part of the duties of enforcement officers, and is likely to be a daily activity. This will <u>not</u> usually require authorisation under RIPA, whether such observation is covert or overt. This is the case even where such observation may be conducted with the aid of a camera or binoculars, provided it does not involve the obtaining of private information. That said, in each and every case, consideration should still be given as to whether the information obtained from using such equipment is to be retained for evidential purposes. Officers should also consider whether the threshold into Intrusive Surveillance has been crossed when using any equipment to enhance their usual sensory perception. If this is the case then the surveillance should be stopped immediately.

5.4 Example**:** Trading Standards Officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out

surveillance of particular individuals. This is part of the general duties of the Council and the obtaining of private information by covert means is unlikely. A directed surveillance authorisation need not be sought.

Use of recording equipment to monitor noise:

5.4 Ordinarily, RIPA cannot be used to authorise covert noise monitoring equipment because the offence of breaching a Noise Abatement Notice is not punishable by a minimum term of imprisonment of 6 months. The revised Home Office Code of Practice provides the following guidance –

- "the covert recording of suspected noise nuisance where; the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm) or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be required"

5.5 The following is provided to offer some general common sense guidance:

- it would not be proportionate to set up noise monitoring equipment to monitor noise from residential property without first taking all other reasonable steps to investigate and bring about a cessation of the nuisance

- if monitoring is inevitable, then where possible the intention to monitor noise should be notified to those who are to be monitored, thereby making any "surveillance" overt

- where giving notice is not possible or where it has not been effective, covert monitoring may be considered a necessary and proportionate option

- in most cases the equipment that is used should only be capable of recognising and recording the frequency levels of noise and incapable of recording anything which would reveal any private information of the inhabitants of the premises being monitored

- where other equipment is used, such as DAT recording, then there is more of a risk that what is being said will also be recorded. Providing that the monitoring is undertaken for the purpose of obtaining noise level readings and is only used at times when noise is considered to be excessive, but which inadvertently, or by the way, might pick up snatches of conversation, then this would not be "directed" surveillance, i.e. surveillance undertaken, "in such a manner 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)"

- the above said, just because the noise is so loud that it can be heard in neighbouring premises does not necessarily mean that the person

causing the noise has forfeited any protection under Article 8 (right to respect for private and family life). Consideration also needs to be given as to whether the surveillance equipment can identify the perpetrators, mindful of the fact that the more sensitive the equipment, the greater the potential for intrusive surveillance, which the Council has no power to authorise

- should you be in any doubt about whether the provisions of RIPA will apply to any surveillance you are planning, you are advised to contact Legal Services (contact details are provided at end of this Manual)

Overt CCTV and ANPR (Automatic Number Plate Recognition) Cameras:

5.6 The provisions of RIPA do not extend to the use of **overt** CCTV surveillance systems, where members of the public are aware that such systems are in operation for their own protection and to prevent crime. Such surveillance does not require authorisation. The operation of CCTV systems is subject to the provisions of the Data Protection Act 1998 and the Council's CCTV Code of Practice. Guidance on the operation of CCTV is provided in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012. Similarly, the overt use of ANPR systems to monitor traffic flow or detect motoring offences does not require an authorisation under RIPA.

5.7 Example: Overt surveillance equipment, such as town centre CCTV systems or ANPR, is used to gather information as part of a reactive operation (e.g. to identify individuals who have committed criminal damage after the event). Such use does not amount to directed covert surveillance as the equipment was overt and was not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.

5.8 In May 2015 there was a further CCTV Code issued by the Information Commissioner's Office (ICO) under the Data Protection Act 1998. This Code is to be considered even if the surveillance is not directed surveillance.

6. Covert use of CCTV

6.1 There may be times when an individual will not be aware that they are the subject of such filming, for instance where the CCTV operator is directed by an investigating officer to carry out surveillance of an individual's movements. The use of the CCTV or ANPR system in these circumstances goes beyond their intended use for general prevention or detection of crime and protection of the public. Such covert surveillance is also likely to be carried out in order to obtain private information (namely, a record of that person's movements and activities). Therefore, in these circumstances, the provisions of RIPA **must** be complied with, and an authorisation for directed covert surveillance should be in place.

7. The Authorising Officer

7.1 The Authorising Officer must be satisfied, that:

a) the surveillance is necessary; and

b) is proportionate to the aim being sought.

7.2 An Authorising Officer should be nominated in each service, and will be responsible for considering all applications for covert surveillance and for granting or refusing authorisations as appropriate. (Authorising Officers may authorise directed covert surveillance to be carried out by any department of the Council). The Authorising Officer will also be responsible for carrying out reviews and ensuring that authorisations are renewed or cancelled where necessary.

7.3 The minimum office, rank or position of an Authorising Officer is designated by Regulation. For a local authority the Authorising Officer must be the Director, Head of Service, Service Manager or equivalent. Within the Council, senior officers, but not so senior that they do not have time to meet all their responsibilities under RIPA, who have been trained to the appropriate level, should be nominated as Authorising Officers.

7.4 All services should also have in place a back-up system for situations where the Authorising Officer is unavailable to grant a written authorisation and the situation becomes urgent. This will enable officers to identify the person who is able to give authorisations in the Authorising Officer's absence.

7.5 Wherever knowledge of confidential information, such as a doctor's report, is likely to be acquired through the directed surveillance, a higher level of authorisation is needed. In the Council, this would be the Head or Paid Service (the Chief Executive) or the person acting as Head of Paid Service in his absence.

7.6 For a list of those officers who have been nominated as Authorising Officers please see App G. It will be the Monitoring Officer's responsibility to retain this list, as well as a list of the back-up officers, and to ensure it is updated periodically.

7.7 The Authorising Officer **must** refuse to authorise any application for surveillance where he/she believes there is insufficient information to assist in making an informed decision on necessity or proportionality, or where there is any question as to whether the proposed surveillance would be lawful. Where this happens, the Authorising Officer must record the reasons for this refusal on the Authorisation Form.

7.8 As all Authorisations need to be signed with an “wet signature” the Monitoring Officer will also keep a record of those signatures against the name of all those who are appointed as Authorising Officers and their back-ups.

Practicalities for the Authorising Officer

7.9 The Authorising Officer should maintain the following documentation, which need not form part of the centrally retrievable record, but which will form part of the Authorising Officer’s own file:

- a copy of the application for authorisation
- a signed copy of the authorisation together with any supplementary documentation, or evidence that the application has been refused/returned to the applicant
- a record of the approval / refusal of Judicial Approval;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- copy of the cancellation form
- copies of all judicial approvals

7.10 The Authorising Officer **must** append a "wet signature" to each authorisation and any subsequent forms (e.g. renewal).

7.11 Whether an authorisation has been granted or refused, the Authorising Officer must scan the relevant forms so that an electronic copy of the completed, signed application and authorisation form can be sent to the coordinating Officer by e-mail, except where the authorisation is for the use of a Covert Human Intelligence Source.

7.12 The coordinating officer must also be sent any reviews or renewals of the authorisation and judicial approvals and the eventual cancellation, so that the central record can be updated accordingly.

8. Necessity and Proportionality

8.1 Obtaining an authorisation in accordance with RIPA will only be a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for directed surveillance to be undertaken.

8.2 The Authorising Officer may only authorise surveillance which is necessary on statutory grounds and s/he must also be satisfied that covert surveillance is necessary in the circumstances of the particular case.

8.3 Once the Authorising Officer has determined that the proposed activities are necessary, s/he must be satisfied that they are proportionate to the overall aim of the investigation.

8.4 Proportionality is a key concept of RIPA and attention must be given to ensure that it is articulated properly. An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve, including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate. Failure to adequately address this issue could see the authorisation falling foul of the RIPA quality procedures, potentially resulting in the surveillance being challenged or suspended.

8.5 This is not just about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, tactic or technique is the least intrusive.

8.6 The activity will not be proportionate if it is excessive in the circumstances of the case or if the information that is being sought could reasonably be obtained by other less intrusive means. As an example of proportionality, a person can claim self-defence to a charge of assault where he has used reasonable force to protect himself - it would be proportionate to kick and punch an assailant armed with a knife but it would not be proportionate to use a knife or a gun against an unarmed attacker.

8.7 All such authorised activities should be carefully managed to meet the objective in question and must not be arbitrary or unfair. Therefore, the Authorising Officer should consider each request for authorisation based only on the facts and reasons given for that particular case on the requisite form.

8.8 In determining whether surveillance is proportionate, the Authorising Officer should make clear that the four elements of proportionality have been fully considered:

(i) balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
(ii) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,
(iii) considering whether the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
(iv) evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

8.9 The bottom line is that the Authorising Officer should set out why s/he <u>believes</u> that the surveillance is necessary and proportionate. A bare assertion is insufficient.

9. Collateral intrusion

9.1 Before authorising any covert surveillance, the Authorising Officer must give consideration to the risk of obtaining private information about persons who are not subjects of the surveillance activity (collateral intrusion). For instance, covert surveillance within a mock auction may result in members of the public being caught on film.

9.2 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to the intrusion into the privacy of the intended subject of the surveillance.

9.3 An application for authorisation should, therefore, include an assessment of the risk of collateral intrusion or interference, and details of any measures taken to limit this, to enable the authorising officer to fully consider the proportionality of the action being proposed.

9.4 Where prior notice/consideration of such collateral intrusion is not possible e.g. where a person who is not the subject of the covert surveillance operation unexpectedly has his privacy compromised, then the officers carrying out the operation should inform the authorising officer as soon as practicable. An example of this would be covert filming outside a night-club, which might unintentionally collect footage of a famous couple together who may not wish it to be known that they were out together.

9.5 In some circumstances this may mean that the original authorisation becomes invalid and a new authorisation may need to be sought, in which case officers should, where practicable, cease the surveillance operation until the authorisation can be corrected/ re-issued.

9.6 Consideration may also have to be given to editing any video evidence that is to be relied upon in court proceedings. It may be advisable in certain circumstances to seek direction from the court about what should or should not be used as evidence and/or disclosed to the Defence or third parties.

10. Collaborative working

10.1 Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the surveillance is to take place and special consideration should be given in cases where the subject of the surveillance or any similar activities being undertaken by other departments of the Council or by other public authorities, which could impact on the deployment of surveillance. Precaution should be taken to ensure that the authorised activity will not be compromised and it is therefore recommended that where an Authorising Officer considers that conflicts might arise they should consult a senior police officer for the area in which the investigation or operation is due to take place.

11. COMMUNICATION DATA

11.1 PSinart I of Chapter II of RIPA relates to the accessing of communications data from service providers. This section does NOT allow for the interception of communications (e.g. bugging of telephones etc). Local authorities are not permitted to intercept the content of any person’s communications and it is an offence to do so without lawful authority

12. Who or What is a Communications Service Provider?

12.1 Communications Service providers (CSP’s) are anyone who provides a service via a telecommunications network – a telephone communications network is the foundation of all telephonic communications be it voice, data, video or internet. Some of the more commonly known examples of service providers are companies such as British Telecom, Orange, Vodaphone, etc.

13 What is communications data?

13.1 The term communications data embraces the 'who', 'when' and 'where' of communication but not the content.
It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on with the communication.

13.2 Communications data is generated, held or obtained in the provision delivery and maintenance of postal or telecommunications services.

13.3 The Council only has power to acquire subscriber information or service use data under Section 21(4)(b) and (c) of RIPA.

13.4 Service use data

This includes:

- Periods of subscription/use
- Itemised telephone call records
- Information about the provision of conference calling, call messaging, call waiting and call barring services
- Itemised timing and duration of service usage (calls and /or connections)
- Connection/Disconnection information
- Itemised records of connections to internet services
- Information about amounts of data downloaded and/or uploaded
- Provision and use of forwarding/redirection services
- Records of postal items e.g. registered, recorded or special delivery postal items
- Top-up details for mobile phones - credit/debit card details and voucher/e-top up details

13.5 Subscriber Information

This includes:

- Name of account holder/ subscriber
- Billing, delivery and installation address(es)
- Contact telephone number(s)
- Bill payment arrangements including bank/credit card details
- Collection/delivery arrangements from a PO box
- Services subscribed to by the customer
- Other customer information such as any account notes, demographic information or sign up data (not passwords)

14. Single Points of Contact

14.1 Service Providers will only respond to requests from Local Authorities via designated single points of contact (SPoC) who must be trained and authorised to act as such. SPoC's should be in a position to:

- Advise applicants if their request is practicable for the service provider
- Advise designated persons as to the validity of requests
- Advise applicants and designated persons under which section of the Act

communications data falls.

14.2 The National Anti Fraud Network (NAFN) provides a SPoC service to the Council precluding the Council from the requirement to maintain their own trained staff and allowing NAFN to act as a source of expertise. All applications for Communication data must be submitted to NAFN who will assist and advice officers and submit the applications to the Designated Person for authorisation.

14.3 Once the application has been approved by a designated person and Judicial Approval has been obtained NAFN, acting as SPOC, will serve a Notice on the relevant service provider requiring the service provider to obtain and provide the information.

14.4 The Act makes provision for the service providers to charge a fee for the provision of information requested and obtained under the Act.

15. Some General Best Practice Points

15.1 The following guidelines should be considered as best working practices with regards to all applications for authorisations covered by this Manual:

- all applications should contain a URN (unique reference number) that is consistently used throughout on all forms relating to that surveillance operation
- applications should avoid repetition of information
- Information contained in applications should be limited to that required by RIPA for directed surveillance authorisations
- an application should not require the sanction of any person other than the Authorising Officer
- where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the application
- authorisations should not generally be sought for activities already authorised either by an application from the Council or another public authority
- where an individual or a non-governmental organisation is acting under the Council's direction, then they are acting as an agent of the Council and any RIPA activities that they are instructed to undertake should be considered for authorisation

16. Duty to report covert activity which was not duly authorised

16.1 All covert surveillance that is not properly authorised should be reported to the Chief Surveillance Commissioner, in writing, as soon as the error is recognised. This includes activity that should and could have been authorised but wasn't or which was not conducted within the directions given by the Authorising Officer. Any such anomalies will normally be picked up at the review stage of an authorisation and if this happens, the Authorising Officer must notify the Monitoring Officer at once.

16.2 This does not apply to covert surveillance which is deliberately *not* authorised because an Authorising Officer considers that it does not meet the legislative criteria but allows it to continue.

16.3 As a matter of good practice, decisions to conduct covert surveillance which cannot benefit from the protection of RIPA should be considered and documented, as much as possible, in line with the RIPA disciplines and checks and balances. However, you should seek advice from Legal Services before embarking on such a course. Such surveillance must still be necessary and proportionate and compliant with the Human Rights Act and should be recorded and authorised by a senior officer.

16.4 Any activity which should have been authorised but was not should be recorded and reported to the Inspectors at the commencement of any inspection to confirm that any direction provided by the Chief Surveillance Commissioner has been followed.

17. Confidential Information (See Chapter 4 of the Revised Home Office Code of Practice on Covert Surveillance and Property Interference)

17.1 There are no special provisions under RIPA for the protection of "confidential information". Nevertheless, special care needs to be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information is involved.

17.2 Confidential Information can include matters that are subject to legal privilege, confidential personal information or confidential journalistic material.

17.3 In practice, it is likely that most of the surveillance authorised and carried out by the Council would not involve confidential information. However, where there is a possibility that the use of surveillance will enable knowledge of confidential information to be acquired e.g. conversations between a doctor and patient, a higher level of authority for such surveillance is required.

17.4 In cases where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation, namely by the Head of Paid Service (Chief Executive) or, in his/her absence, the Chief Officer acting as Head of Paid Service.

17.5 The Applicant should complete the application for authorisation of directed surveillance in the usual way, but with sufficient indication of the likelihood that confidential information will be acquired.

18. Communications subject to Legal Privilege

18.1 Communications between professional legal advisers and their client or persons representing their client can attract legal privilege if they are:

(a) made in connection with the giving of legal advice to the client; and
(b) made in connection with or in the contemplation of legal proceedings or for the purpose of such proceedings

18.2 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose, regardless of whether the lawyer is acting unwittingly or culpably.

18.3 As stated, there is no special protection afforded to legally privileged information. However, such information is particularly sensitive and surveillance which uncovers such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8.

18.4 It is extremely unlikely that legally privileged material obtained by directed surveillance would ever be admissible as evidence. Moreover, just the mere fact that this type of surveillance has taken place may lead to any related criminal proceedings being stayed for abuse of process.

18.5 If the covert surveillance is not intended to result in the acquisition of knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it. If the risk cannot be removed entirely, the application should explain what steps will be taken to ensure that any knowledge of matters subject to legal privilege which is obtained is not used in any investigation or prosecution.

18.6 Where covert surveillance is likely to or intended to result in the acquisition of legally privileged information, a higher level of authorisation (i.e. Head of Paid Service) is required as for Confidential Information. That said, the authorising Officer must also be satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life and limb, or national security, and he surveillance is reasonably regarded as likely to yield intelligence necessary to counter that threat.

18.7 Furthermore, in those cases where legally privileged material has been acquired and retained, the matter should be reported to the Authorising Officer by means of a review and to the relevant Commissioner or Inspector during his next inspection, at which the material should be made available if requested.

19. Legal Consultations

19.1 Following several high-profile cases where legally privileged information was acquired through covert surveillance directed in places where legal consultations were taking place, there has now been a significant change in regime.

19.2 The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 provides that directed surveillance that is carried out in relation to anything taking place on specified premises used for the purposes of “legal consultations” shall be treated for the purposes of RIPA as *intrusive surveillance.*

19.3 Locations specified under the 2010 Order include prisons, police stations, cells at Magistrates' courts as well as the place of business of any professional legal adviser.

19.4 As has already been mentioned, the Council has no lawful power to authorise or carry out intrusive surveillance.

19.5 If in doubt as to whether the planned surveillance is likely to involve confidential information, or more importantly, legal privilege, please contact the Contentious Law team. (Contact details can be found at the end of this Manual).

20. Information to be included in Applications for Authorisation

20.1 A written application for authorisation for Directed Surveillance should describe the conduct to be authorised and the purpose of the investigation or operation. It should also include:

- the reason why the surveillance is necessary;
- the reasons why it is proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance;
- a subsequent record of whether the authorisation was given or refused, by whom and the date and time.

20.2 The Applicant officer must obtain the requisite form from the Monitoring Officer. This means that as soon as an officer believes it is necessary to deploy covert surveillance to achieve the aims of his investigation, he should email the Monitoring Officer and request an Application Form. The Monitoring Officer will also allocate the form with the next sequential Unique Reference Number (URN).

20.3 An example of the application for authorisation of directed surveillance form is attached to this Code (see Appendix A).

21. Authorisation Form

21.1 The completed Application form should be given to the Authorising Officer. The Authorisation form is the only document which should be reviewed by a court during a trial where a dispute arises as to whether evidence obtained by way of covert surveillance was obtained lawfully. Therefore, this document must include all relevant information to ensure it can be presented as a stand-alone document to justify why the surveillance has been undertaken.

21.2 The Authorising Officer should, therefore, record on the Authorisation form the full extent of what is authorised i.e. who, what, why, when, where and how, including an independent authorisation for any technical equipment which is to be used and the location of such equipment. This will ensure that the specific parameters of what has been duly authorised is then passed to the Applicant/ officer carrying out the surveillance. The Authorising Officer should also explain why he is satisfied that the directed surveillance is necessary and proportionate in the circumstances of the case, before he endorses the Authorisation.

21.3 The Authorising Officer must check that the Authorisation Form sent by the Monitoring Officer includes the same URN as appears on the Application Form.

21.4 As mentioned above, if the authorisation is refused, the Authorising Officer should clearly mark on the form the reasons for refusal and any comments that may assist the Applicant Officer to reconsider the proposals and resubmit a fresh application. Copies of such refusals must also be sent electronically to the Monitoring Officer.

21.5 An example of the Authorisation form is included with this Manual as Appendix B.

21.6 Should the use of evidence obtained by way of Directed Surveillance be challenged in any subsequent prosecution then the Council will only need to disclose the Authorisation Form as proof that the requisite authority was obtained in accordance with RIPA. This will mean that any confidential information or intelligence that may have been included in the Application form is likely to be protected from disclosure.

22. Duration of authorisations

22.1 A written authorisation for Directed Surveillance is initially valid for three months from the day on which it took effect, i.e. from the date of Judicial Approval, but can be renewed within that time, though any renewal will require judicial approval.

23. Reviews

23.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

23.2 In each case the relevant Authorising Officer should determine how often a review should take place during the lifetime of any authorisation and should then undertake the review him/herself.

23.3 Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in the further or greater intrusion into the private life of any person, should also be bought to the attention of the

Authorising Officer by means of a review. The Authorising Officer should consider whether the proposed changes are proportionate before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

23.4 Where a directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a review to include the identity of these individuals. It would also be appropriate to convene such a review for this purpose.

Example: directed surveillance authorisation is obtained to authorise surveillance of X and his associates for the purpose of investigating their suspected involvement in a crime. X is seen meeting with A and it is assessed that subsequent surveillance of A will assist the investigation. Surveillance of A may continue, but the directed surveillance authorisation should be amended at a review to include "X and his associates, including A".

23.5 Again, the Authorising Officer should request a review form from the Monitoring Officer. An example of the review form is attached to Manual as Appendix C.

24. Renewals

24.1 An authorisation may be renewed for a further period of three months, if the Authorising Officer considers it necessary for the authorisation to continue. However, renewal will be subject to judicial approval, as described above.

24.2 Authorisations may be renewed more than once, provided the same grounds for surveillance still apply and the surveillance continues to be proportionate to the aims seeking to be achieved.

24.3 All requests for renewals should record:

- whether it is the first renewal, if not list all previous occasions when renewed;
- any significant changes to the information given in the original authorisation;
- the reasons why it is necessary to continue with the surveillance and that it is still proportionate to the aim being sought;
- the content and value to the investigation or operation of the information so far obtained by surveillance;
- the results of regular reviews of the investigation or operation

24.4 The Authorising Officer should request a review form from the Monitoring Officer. The renewal form is attached to this Manual as Appendix D.

25. Cancellations

25.1 If, during the currency of an authorisation, the Authorising Officer is satisfied that the authorisation is no longer necessary, s/he must cancel it. It is a

statutory requirement that authorisations are cancelled as soon as they are no longer required. Judicial Approval is not required to cancel an authorisation.

25.2 As soon as the decision is taken to cancel the authorisation, the Authorising Officer must inform those carrying out the surveillance and the date and time of this notification should be recorded on the Cancellation Form.

25.3 A Cancellation Form must be completed in all cases, whether the authorisation is being cut short for want of necessity or whether it has run its full course and the surveillance has been completed. This is to ensure that the Authorising Officer has given consideration to the product of such directed surveillance, and has given the necessary direction as to the handling, retention and/or destruction of such product.

25.4 Cancellations should also include the reason for cancellation as well as the result of the operation, and they must also be noted on the central record of authorisations.

25.5 Again, the Authorising Officer should request a cancellation form from the Monitoring Officer. The cancellation form is attached to this Manual as Appendix E.

25.6 See Appendix F for a flowchart to assist in determining whether the activity you are considering to undertake is directed surveillance.

26. Surveillance carried out by a third party

26.1 There will be instances when the Council employs a third party, such as a security firm, to install covert cameras for the purpose of directed surveillance. It is still the responsibility of the Council to ensure that the necessary authorisation has been obtained before such a contract can be carried out.

26.2 Likewise, where for instance the police request the use of the Council's CCTV system for covert surveillance of an individual/s then the police should ensure they have the requisite authorisation to present to the Council, before such surveillance is carried out (except in cases of urgency). Although the equipment being used belongs to the Council, it is the police who are directing the surveillance and they are ultimately responsible.

26.3 In any case where the surveillance is to be carried out by someone other than the Applicant officer, whether that is through a security firm or by Council Officers in a different department (e.g. CCTV controllers) then those carrying out the surveillance must be given the exact wording and parameters of the surveillance that has been authorised. There should be a written contract setting out the parameters and the need to comply with RIPA, the Data Protection Act 1998 and the Human Rights Act, where applicable.

26.4 The easiest way for this to be achieved is by handing a copy of the authorisation to the surveillance officer, although where the surveillance does not involve the installation of devices it will be sufficient for the officer in charge of the surveillance team to see the documents and then brief the team accordingly, taking care to repeat the precise form of words used by the

Authorising Officer. In each case the officer carrying out the surveillance should endorse the authorisation form to show they have understood what is expected of them.

26.5 It is also imperative that a cancellation form is provided to the third party who has been carrying out the surveillance, as soon as there is no longer a necessity for the surveillance and/or the requisite information has been obtained:

- If the surveillance was initially authorised by the Council then the cancellation form should be completed by the Authorising Officer and a copy should be sent to the Monitoring Officer to store on the Central Record, and

- If the Council's CCTV control room has been tasked with carrying out covert surveillance on behalf of another public authority e.g. the police then the staff in the control room will make regular checks to see whether the surveillance is still "live" and with ensure that a copy of the requisite cancellation form is provided to them once the surveillance comes to an end.

27. Obtaining Judicial Approval

From 1st November 2012 judicial approval of all local authority authorisations and renewals (for both directed covert surveillance and the use of a CHIS), is required from the Magistrates' Court. Authorisations and renewals are invalid and cannot be acted upon until the approval of the Court has been given.

27.1 The Magistrates' Court may give approval only if it is satisfied that –

- authorisation is necessary for the prevention or detection of crime; and
- that authorised surveillance would be proportionate to what is sought to be achieved by carrying it out; and;
- the authorising officer was an individual designated for the purpose, i.e. Director, Head of Service, Service Manager, or equivalent; and
- the crime being investigated carries a minimum prison sentence of 6 months, or concerns the sale of alcohol to children, or allowing the sale of alcohol to children, or persistently selling alcohol to children, or selling tobacco to children; and
- at the time of the application to the Magistrates' Court there remains reasonable grounds for believing that the above conditions are met

27.2 The Council is not required to give notice of the intended application to the Magistrates' Court of the application to the person to whom the authorisation relates, or to such a person's legal representatives.

Making the Application

27.3 After an application has been authorised by the designated officer, the investigating officer should contact Westminster Magistrates' Court to arrange a hearing. The authorising officer should provide the Court with a copy of the original application, the authorisation and any supporting documents setting

out the case. In addition, the investigating officer should provide the Court with a partially completed judicial application / order form (see Appendix K). This forms the basis of the application to the Court and should contain all information that is relied upon. The original RIPA authorisation or notice should be shown to the Justice of the Peace, but should be retained by the Council 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.

27.4 Although the investigating officer is required to provide a brief summary of the circumstances of the case on the judicial application form, this does not replace the need to supply the original RIPA authorisation as well. The order section of the form will be completed by the Court and will be the official record of the Court's decision. The Council will retain all original paperwork associated with applications for Judicial Approval. There is no requirement for the Court to consider either cancellations or internal reviews.

Arranging a Hearing

27.5 On the rare occasion where out of hours access to a Justice of the Peace is required then it will be for the investigating officer to make arrangements with Westminster Magistrates' Court. In these cases the investigating officer will need to provide two partially completed judicial application / order forms so that one can be retained by the Court. The investigating officer should provide the court with a copy of the signed judicial application / order form the next working day.

27.6 In most emergency situations where the police have power to act, then they should be able to authorise activity under RIPA without prior Judicial Approval. RIPA authority is not required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

27.7 Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the investigating officer's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

Attending a Hearing

27.8 The hearing is a 'legal proceeding' and therefore **local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the Court**. Investigating officers should contact Legal Services.

27.9 The hearing will be in private and heard by a single Justice of the Peace who will read and consider the RIPA authorisation and the judicial application / order form. He / she may have questions to clarify points or require additional reassurance on particular matters.

Decision

27.10 The Justice of the Peace will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met. If more information is required to determine whether the authorisation or notice has met the tests then the Justice of the Peace will refuse the authorisation. If an application is refused the Council should consider whether we can reapply, for example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

Outcomes

27.11 Following consideration of the case the Justice of the Peace complete the order section of the judicial application / order form recording his / her decision. The various outcomes are detailed below –

The Justice of the Peace may decide to -

Approve the Grant or renewal of an authorisation

- The grant or renewal of the RIPA authorisation or notice will then take effect and the Council may proceed to use the technique in that particular case

Refuse to approve the grant or renewal of an authorisation

- The RIPA authorisation will not take effect and the Council may not use the technique in that case. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the Council having to go through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those steps have been taken

Refuse to approve the grant or renewal and quash the authorisation

- This applies where the Court refuses to approve the grant or renewal of an authorisation and decides to quash the original authorisation. The court must not exercise its power to quash the authorisation unless the Council has had at least 2 business days from the date of the refusal in which to make representations.

27.12 When an application for judicial approval is refused, the Magistrates' Court will make an order quashing the authorisation.

27.13 All forms required to be completed at the various stages of the process will be held by the Monitoring Officer. Requests for forms should be made by email to the Knowledge and Information Management Team at RIPA@westminster.gov.uk

28. Central Record of all authorisations / Role of the RIPA Coordinating Officer

28.1 A record of the following information pertaining to all authorisations shall be centrally retrievable for a period of at least five years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, reviewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request:

- the type of authorisation
- the date the authorisation was given
- name and rank/grade of the authorising officer
- the unique reference number (URN) of the investigation or operation
- the title of the investigation or operation, including a brief description of the names of subjects, if known
- details of attendances at the magistrates' court
- the dates of any reviews
- if the authorisation had been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer
- whether the investigation or operation is likely to result in obtaining confidential information as define din the Home Office Code of Practice
- whether the authorisation was granted by an individual; directly involved in the investigation
- the date the authorisation was cancelled

28.2 the following documentation should also be centrally retrievable for at least five years from the ending of each authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer
- a record of the period over which the surveillance the surveillance has taken place
- the frequency of reviews prescribed by the authorising officer
- a record of the result of each review of the authorisation
- a copy of any renewal of an authorisation. Together with the supporting documentation submitted when the renewal was requested
- the date and time when any instruction to cease surveillance was given
- the date and time when any other instruction was given by the authorising officer
- a copy of the order approving the grant or renewal from a Justice of the Peace (JP)

28.3 The central record kept by the Council includes hyperlinks to each and every document in the authorisation process. This is not only to enable compliance with the necessary requirements but also to assist the coordinating Officer to carry out quality control.

28.4 Therefore, all authorisations granted by individual Authorising Officers, on behalf of the Council, must be sent electronically to the coordinating Officer.

28.5 The coordinating officer will be responsible for updating this record whenever an authorisation is granted, renewed, reviewed or cancelled. This record must be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request.

29. Quality Control

29.1 The co-ordinating officer will also be responsible for maintaining a central quality control of all authorisations. This will entail monitoring the authorisations for any inconsistencies and checking each authorisation to ensure that the Authorising Officer has clearly addressed his/her mind to the statutory requirements of necessity and proportionality in each case.

29.2 The coordinating officer should reject any authorisation where there is insufficient evidence that the Authorising Officer has carefully considered these statutory requirements before granting the authorisation. The Monitoring Officer should also ensure that all authorisations have been signed with a “wet signature”.

29.3 The coordinating officer will also send reminders to Authorising Officers when a review is pending or a renewal will be necessary. Please see Appendix H for a Flow Chart identifying the required documentation at each stage of the RIPA process.

30. The Unique Reference Number (URN)

30.1 The coordinating Officer will be responsible for providing the URN on the initial Application Form as well as ensuring that it is recorded on the Authorisation Form and subsequent forms completed in the process. This will ensure sequential numbering of unique numbers and provide insurance that all covert activity is captured by the central record rather than relying on notification by the Authorising Officer alone.

30.2 The URN should also provide sufficient information to be able to identify at a glance which department the authorisation derives from and also the number of authorisations that have been granted by that department. For instance 4/TS/1/09 denotes that the fourth entry on the central record is an authorisation from Trading Standards and is the first one by that service in 2009.

30.3 The following is a list of codes to be used by departments for their URNs:
Au – Audit
CWH (Estate Office) – City West Homes followed by ref to which estate office the authorisation derives from

EH (F) – Environmental Health (Food Team)
EH (R) – Environmental Health (Residential)
H&S – Health & Safety Team
PM – Premises Management
SM – Street Management
Lic – Licensing
NT – Noise team
PET – Planning Enforcement Team
TS – Trading Standards

31. Retention and destruction of surveillance footage

31.1 Where surveillance footage could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements.

31.2 Particular attention is also drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

31.3 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance.

31.4 Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

31.5 The Authorising Officer also needs to include an explanation of what will happen to the surveillance product on the cancellation of each and every authorisation.

31.6 Further guidance on the storage, retention and destruction of surveillance footage can be found in the Council's CCTV Code of Practice. Copies of this document can be requested from the Neighbourhood Crime Reduction Team.

32. Covert Human Intelligence Sources

32.1 A person is a Covert Human Intelligence Source (or CHIS) if:

(i) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating anything falling within (ii) and (iii) below;

(ii) he covertly uses the relationship to obtain information or to provide access to any information to another person; or

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

32.2 It is also important to note that an individual who provides information to the Council voluntarily may become a CHIS, e.g. where a member of the public covertly provides the Council with information which has been obtained in the course of, (or *as a consequence of the existence of* – s. 26(8)(c) RIPA), a personal or other relationship, such as a neighbour or relative of a suspected offender. Such an "informant" may be at risk of reprisals, and would be a person to whom a duty of care would be owed if the information was used. Where information is provided on one occasion without request, a CHIS situation is unlikely to apply, but should the provision of information continue, even where the information has not been requested, the member of the public might very well become a CHIS and could require authorisation. Alternatively, an instruction to the member of the public to cease providing the information could be given. This will be a matter of judgement on a case by case basis.

32.3 It is important to recognise the difference between "establish" and "maintain". "Establishes a relationship" means to "set up a relationship". It does not require endurance over a period of time, as does, "maintain", so it could apply to a situation involving a seller and purchaser concerning a single transaction. Most one-off test purchases would not require a CHIS authorisation, but where the duration and nature of the test purchase is out of the ordinary, then a CHIS authorisation may be necessary, e.g. where two officers pose as a couple wishing to purchase a time-share property / an engagement ring, in circumstances where they desire the seller to believe their "cover" and to trust that they are who they say they are; where they are likely to have to enter into conversations aside from a simple request to purchase goods and where the nature and endurance of the face to face test purchase is such that the officers intend to establish a relationship whereby the seller feels at ease and confident to behave in a particular way.

32.4 Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain information.

32.5 An authorisation is needed for the **use** or **conduct** of a CHIS. Although these appear at first to be the same thing, and indeed most CHIS authorisations will be for both use and conduct, there is a very subtle difference:

- The "conduct" of a CHIS is any conduct which falls within 7.1 above. In other words, an authorisation for conduct will authorise steps taken by a CHIS, on behalf of, or at the request of, the Council.

- The "use" of a CHIS involves any action on behalf of the Council to induce, ask or assist a person to engage in the said conduct of a CHIS, or to obtain information by means of that conduct.

32.6 The purpose will only be covert if the relationship referred to above is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose, or unaware of the use of or disclosure of any such information.

32.7 Therefore, a straightforward test purchase would not give rise to a CHIS situation:

Example1: a young person purchasing a packet of cigarettes / alcohol where the conversation is restricted to the ordering, acceptance and payment for the goods. (**Note:** authorisation for directed surveillance would be required if it is intended that the young person should carry a concealed camera / microphone, or is being watched by an enforcement officer)

Example 2: an enforcement officer purchasing theatre tickets as above. (**Note**: authorisation for directed surveillance would be required where it is intended that the officer should carry a concealed camera / microphone)

32.8 However, a CHIS situation might very well arise where officers pose as a consumer / retailer and seek to gain a person's trust, in order to obtain evidence of criminal offences. Examples include:

- posing as a retailer at a wholesale outlet which is believed to sell counterfeit goods, where the test purchase might involve gaining the trust of the seller, in order to ascertain what can be supplied and to agree terms of sale

- posing as a consumer at a hair loss treatment centre where false or misleading claims may be made to vulnerable consumers

- posing as a customer in a lap dancing club, entering into conversation with the dancers / buying them drinks and paying for personal / private dances

32.9 The above scenarios give rise to an understanding or element of trust between the parties: something more than a straightforward request to supply or sell goods and services.

Note: officers must <u>never</u> act as an agent provocateur by attempting to persuade or encourage an individual to commit an offence that he would not otherwise commit. It is one thing to ask questions of an individual to ascertain information about what is being offered, i.e. "so how many bottles of Chanel No.5 perfume could you supply by Friday?" but quite another to attempt to persuade a trader to meet such a request after he has stated, e.g. that he only sells clothing wholesale and is unable to supply perfume

32.10 The Council should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly, without obtaining a CHIS authorisation.

32.11 CHIS scenarios at Westminster are few and far between. As soon as the officer *believes* the need for an authorised CHIS has been established, the lead enforcement officer should contact Legal Services who will guide the officer through the process.

General rules on Authorisation of a CHIS

32.12 This type of covert surveillance requires authorisation by an Authorising Officer in the same way as for Directed Surveillance, and the procedure for making an application for authorisation is, broadly speaking, similar to that for Directed Surveillance, including the fact that an authorisation may only be granted where such surveillance is necessary on one of the statutory grounds; that any such use of a CHIS must be reasonable and proportionate, and that due consideration should be given to collateral intrusion. Judicial approval is also required.

32.13 The Authorising Officer will be the same officer who would authorise covert surveillance – see appendix G (NB: the authorising officer should not also be the Handler).

32.14 A written Authorisation lasts for 12 months except in the case of juveniles. It can be renewed for a longer period provided the use or conduct of the CHIS is still reasonable, necessary and proportionate. In practice, the Council is unlikely to deploy a CHIS for anywhere near this length of time and so the Authorising Officer should ensure that regular reviews are carried out and that the authorisation is cancelled as soon as the CHIS is no longer necessary. In some cases the safety and welfare of the CHIS should continue to be taken into account after cancellation.

32.15 An authorisation for the use or conduct of a CHIS will provide lawful authority for any such activity that:

- Involves the use or conduct of a CHIS as is specified or described in the authorisation;
- Is carried out by or in relation to the person to whose actions as a CHIS the authorisation relates; and
- Is carried out for the purposes of, or in connection with, the investigation or operation so described.

32.16 It is therefore vital that the CHIS, as well as those involved in the use of a CHIS, are aware of the extent and limits of any conduct authorised.

Local considerations and Community Impact Assessments

32.17 Any person applying for or granting an authorisation will also need to be aware of any particular sensitivities in the local community where a CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS.

32.18 Where an authorising officer considers that a conflict might arise they should, where possible, consult with a senior officer from the City of Westminster Police. The Council, where possible, should also consider consulting other relevant public authorities to gauge community impact.

Use of CHIS with technical equipment

32.19 An authorised CHIS wearing or carrying a surveillance device does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of that CHIS. However, if that is not the case, and the device will be used other than in the presence of the CHIS then the relevant authorisation will be needed. In respect of the Council, such use can only be within the public domain, for which a directed surveillance authorisation should be obtained, given that a local authority has no power to grant an authorisation for intrusive surveillance.

32.20 That said, a CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in his presence. This also applies to the recording of telephone conversations or other forms of communication, other than by interception, which takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way.

Oversight of use of a CHIS by the local authority

32.21 The requirement for elected members of the Council to review the use of RIPA every 12 months and to set the policy, referred to earlier in this Manual, includes the use of a CHIS.

Management of CHISs

32.22 As well as being satisfied that the authorisation is necessary for the purpose of preventing or detecting crime or of preventing disorder and that the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use, an Authorising Officer shall not grant an authorisation for the conduct or use of a covert human intelligence source unless he believes that there are arrangements in place as are necessary for ensuring:

(a) that there will at all times be a person who will have day-to-day responsibility for dealing with the source on behalf of the Council and for the source's security and welfare. This person is known as the Handler and is responsible for dealing with the CHIS on behalf of the authority; directing the day to day activities of the CHIS; recording the information supplied by the CHIS and monitoring the CHIS's security and welfare. The handler would usually hold a rank or position lower than the authorising officer;

(b) that there will at all times be another person who will have general oversight of the use made of the source. This person is known as the Controller and will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS. Obviously, this must be someone other than the Handler and ideally should be someone other than the authorising officer, but due to the relatively small size of the Council's enforcement teams, the authorising officer is likely to be the Controller.

(c) that there will at all times be a person who will have responsibility for maintaining a record of the use made of the source. This will be the responsibility of the Handler.

(d) that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters as are specified in regulations made by the Secretary of State, (see below); and

(e) that records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

Particulars to be contained in records

32.23 The Secretary of State has made the Regulation of Investigatory Powers (Source Records) Regulations 2000. The following particulars must be included in the records relating to each source:

(a) the identity of the source;

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

(c) any relevant investigating authority other than the authority maintaining the records;

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

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

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

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

(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

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

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

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

(l) the information obtained by each relevant investigating authority by the conduct or use of the source;

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

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

Security and Welfare

32.24 The Council should also take into account the safety and welfare of any CHIS it deploys, when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use of that CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. As previously mentioned, the ongoing safety and welfare of the CHIS, after cancellation of the authorisation, should also be considered at the outset.

32.25 Also consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of the CHIS to, or in, court.

32.26 The CHIS Handler is responsible for bringing to the attention of the CHIS Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

32.27 Where appropriate, concerns about such matters must be considered by the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

32.28 For further information about the centrally retrievable store of information, the retention and destruction of material, the Senior Responsible Officer and handling complaints, see the relevant sections of the Manuel.

33. RIPA Coordinator

33.1 It is established best practice that all authorisations should be held in a central record and that a RIPA Coordinator will be responsible for maintaining that record as well as carrying out a quality control function on all authorisations. The central record will be held by the Knowledge and Information Management Team and the RIPA coordinator functions for the Council will be carried out by the Corporate Information Manager, who is the manager of that team.

34. Senior Responsible Officer and the role of Councillors

34.1 It is recommended best practice that there should be a Senior Responsible Officer (SRO) in each public authority who is responsible for:

- the integrity of the processes in place to authorise directed surveillance;
- compliance with RIPA and with the Codes of Practice;
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

34.2 As the SRO for a local authority has to be a member of the corporate leadership team, and in light of the SRO's responsibilities, the Senior Responsible Officer for Westminster Council will be the Head of Legal Services. He will also be responsible for ensuring that all authorising officers are of an appropriate standard in light of the recommendations or concerns raised in the inspection reports prepared by the Office of Surveillance Commissioners following their routine inspections.

34.3 The SRO will also undertake an annual audit of records but will not be responsible for the day-to-day quality control which will still be within the remit of the RIPA coordinator.

34.4 There is also now a requirement for elected members of the Council to review the use of RIPA and to set the policy on covert surveillance at least once a year. Therefore, the Policy and Scrutiny Committee will review this Manual as well as the Policy every 12 months and will report to Cabinet, should they be of the opinion that it is not fit for purpose.

34.5 The Policy and Scrutiny Committee will also consider the Council's use of RIPA every 6 months to ensure that it is being used consistently with the Council's Policy and Procedure Manual. Should the Committee be concerned by any adverse trends disclosed in the reports it receives, it should call for reports every quarter.

34.6 The Committee should not, and will not, be involved in making decisions on specific authorisations.

35. Training

35.1 Both Authorising Officers and those applying for authorisations should attend regular training sessions to ensure they are being kept up-to-date with any developments, both procedurally and legally.

35.2 The RIPA coordinator will be responsible for keeping a record of training that has been provided across the Council and CityWest Homes, and will also help to co-ordinate relevant training sessions for the appropriate officers.

36. Complaints

36.1 There is provision under RIPA for the establishment of an independent Tribunal. This Tribunal will be made up of senior members of the legal profession or judiciary and will be independent of the Government.

36.2 The Tribunal has full powers to investigate and decide upon complaints made to them within its jurisdiction, including complaints made by a person who is aggrieved by any conduct to which Part II of RIPA applies, where he believes such conduct to have taken place in "challengeable circumstances" or to have been carried out by or on behalf of any of the intelligence services.

36.3 Conduct takes place in "challengeable circumstances" if it takes place:

(i) with the authority or purported authority of an authorisation under Part II of the Act; or

(ii) the circumstances are such that it would not have been appropriate for the conduct to take place without authority; or at least without proper consideration having been given to whether such authority should be sought.

36.4 Further information on the exercise of the Tribunal's functions and details of the relevant complaints procedure can be obtained from:

Investigatory Powers Tribunal

PO Box 33220
London
SW1H 9ZQ

020 7273 4514

36.5 Notwithstanding the above, members of the public will still be able to avail themselves of the Council's internal complaints procedure, where appropriate, which ultimately comes to the attention of the Local Government Ombudsman.

37. The Office of Surveillance Commissioners

37.1 The Act also provides for the independent oversight and review of the use of the powers contained within Part II of RIPA, by a duly appointed Chief Surveillance Commissioner.

37.2 The Office for Surveillance Commissioners (OSC) was established to oversee covert surveillance carried out by public authorities and within this Office an Inspectorate has been formed, to assist the Chief Surveillance Commissioner in the discharge of his review responsibilities.

37.3 One of the duties of the OSC is to carry out planned inspections of those public authorities who carry out surveillance as specified in RIPA, to ensure compliance with the statutory authorisation procedures. At these inspections, policies and procedures in relation to directed surveillance and CHIS operations will be examined and there will be some random sampling of selected operations. The central record of authorisations will also be inspected. Chief Officers will be given at least two weeks' notice of any such planned inspection.

37.4 An inspection report will be presented to the Chief Officer, which should highlight any significant issues, draw conclusions and make appropriate recommendations. The aim of inspections is to be helpful rather than to measure or assess operational performance.

37.5 In addition to routine inspections, spot checks may be carried out from time to time.

37.6 There is a duty on every person who uses the powers provided by Part II of RIPA, which governs the use of covert surveillance or covert human intelligence sources, to disclose or provide to the Chief Commissioner (or his duly appointed Inspectors) all such documents and information that he may require for the purposes of enabling him to carry out his functions.

IMPORTANT NOTE

This Procedure Manual has been produced as a guide only and is primarily based on the revised Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources published by the Home Office. These Codes can be found at www.homeoffice.gov.uk

Legal Services
March 2016