ENFIELD COUNCIL

COVERT SURVEILLANCE PROCEDURES

IN ACCORDANCE WITH THE REGULATION OF INVESTIGATORY POWERS ACT 2000

This manual should be read in conjunction with the codes of practice (Covert Surveillance and Property Interference and Covert Human Intelligence Sources), which provide additional guidance for officers who undertake covert surveillance.

CONTENTS

1. Introduction

Background

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") regulates the way the following investigations are carried out: for the prevention and detection of crime.

i) Directed Surveillance (DS)
ii) Covert Human Intelligence Sources (CHIS)
iii) Access to Communications Data

The Council may only carry out these operations for the purpose of detecting or preventing crime. The crime involved for DS must be 'serious' which means that it must carry a maximum sentence of at least 6 months.

RIPA was introduced to limit the investigatory powers of public bodies in order to comply with the Human Rights Act 1998. In particular, public bodies must take into account the public's right to private and family life and any investigation which interferes with this right must be weighed against the need to detect and prevent crime for each individual case.

The Codes of Practice

1.2 The Codes of Practice as amended (Covert Surveillance and Property Interference and Covert Human Intelligence Sources) were issued in accordance with section 71 of RIPA and are admissible as evidence in a court of law. Following these procedures will assist officers in ensuring compliancy with the codes.

Scope of Surveillance Activity

1.3 RIPA permits public authorities to undertake covert surveillance where it is likely to result in the obtaining of private information about a person.

1.4 Surveillance includes monitoring, observing or listening to persons including their movements, conversations or other activities. Surveillance may or may not involve the use of devices such as CCTV cameras.

1.5 Covert Surveillance 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.

1.6 Covert Surveillance governed by RIPA falls into two domains:

- Directed Surveillance; and
- Intrusive Surveillance.

All officers must observe that **the council is not permitted to undertake intrusive surveillance** and understand where the boundary lies between these activities. Intrusive surveillance will be referenced in these procedures for the sole reason of preventing officers from unknowingly undertaking such activities.

Considerations for Lawful Surveillance Activity

1.7 As already mentioned covert surveillance interacts with other legislation that protects an individual's right for privacy (article 8 of the ECHR). In addition Article 6 of the ECHR, the right to a fair trial, may also be relevant where a prosecution follows the use of covert methods.

1.8 Furthermore evidence which relies on covert surveillance may be deemed inadmissible by a court of law if the obtaining of it contravenes the Police and Criminal Evidence Act 1984.

1.9 Covert Surveillance will potentially involve the processing of personal data and therefore the Data Protection Act 1998 must be complied with to ensure that data is processed in accordance with the Data Protection Principles.

1.10 RIPA provides a statutory framework under which covert surveillance activity can be conducted lawfully and in harmony with the other legislation referred to above. By following these procedures officers can reduce the risk of the Council being liable to pay compensation for breach of Human Rights. Similarly it will reduce the possibility of a complaint being made to the RIPA Tribunal (see Section 9). Failure to follow the codes of practice will attract criticism from the Investigatory Powers Commissioner's Office who periodically inspect the practices of public authorities (see Section 10)

1.11 By adhering to these procedures the council will be afforded a shield to defend itself against a claim that it has used its powers for covert surveillance unlawfully and in breach of individuals' rights to privacy.

2. Definitions of Directed Surveillance and Intrusive Surveillance

2.1 **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); but
c) not in a situation where the activity is an immediate response to events or circumstances.

2.2 **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.

The Council is **NOT** permitted to undertake this method of surveillance.

Private Information

2.3 For the purposes of covert surveillance private information includes information relating to a person's private and family life, and extends to include professional and business activities.

2.4 It should be noted that even when conducting covert surveillance in a public place most information obtained, where the individual had some expectation of privacy, is 'private information'

Example: Two people, including the subject of an investigation, having a discussion in a restaurant will have an expectation of privacy regarding the contents of that discussion, even if they are in a public place. Therefore if the council wished to monitor and listen in on the conversation an authorisation for Directed Surveillance should be sought.

2.5 Careful consideration should be given when using historical information in order to establish a pattern of behaviour or to learn something about a person's relationships. In isolation these fragments of information may not avail anything of consequence but when examined in the whole serves to reveal personal information about the individual. Such an activity can be construed as requiring authorisation for Directed Surveillance.

Example: Officers of a local authority examine CCTV footage for specific locations within a given time frame to establish the location of an individual or individuals as part of an investigation. The CCTV footage was not originally intended to be used for this specific purpose and therefore a Directed Surveillance authorisation would be appropriate for the examination of the footage for the purposes of this investigation.

Exemptions from Requiring Authorisation

2.6 Certain surveillance activities are not to be treated as Directed Surveillance for the purposes of RIPA and therefore no authorisation is deemed necessary. Such activity includes the following:

Immediate Response to Events

2.6.1 Covert surveillance that is carried out by way of an immediate response to events, the nature of which is such that it is not reasonably practicable to obtain authorisation under RIPA, would not require a Directed Surveillance authorisation. Such surveillance, although it may be covert, is nevertheless not Directed and therefore no authorisation for Directed Surveillance is necessary.

2.6.2 A response is not to be regarded as “immediate” because of the neglect in the need for an authorisation which was left too late to apply for.

Routine Observation Activity

2.6.3 Where officers are performing covert activities as part of their routine duties, they would not require authorisation under RIPA. This is because this is not an operation targeting individuals; it is merely carrying out an ordinary duty to detect crime.

Example: Trading Standard Officers conducting a routine observation of a car boot sale and monitoring whether particular counterfeited products such as computer console games are being sold as genuine items. No Directed Surveillance authorisation is necessary.

Overt and Covert use of CCTV and ANPR Cameras

2.6.4 In the situation where the public are aware that CCTV and ANPR systems are operating for legitimate purposes, such (overt) surveillance does not fall into the scope of Directed Surveillance and does not require an authorisation under RIPA. However where covert use of such systems are employed, to determine an individual’s movements for instance, this then may become Directed Surveillance as it goes beyond the primary, overt, use of prevention or detection of crime and an authorisation should be sought.

The use of “Hot Lists” when employing these technologies to monitor vehicles over a stretch of public road for crime related purposes may require consideration for an authorisation. This will be largely dependent on the purpose of the list and also the action that is taken when the vehicle or persons are observed. Specifically, if the purpose of the list is for a particular investigation or if the targets have a propensity to commit crime and then when observed the movements are monitored or collected for analysis this will require an authorisation. It is therefore clear that there is a need to keep separate lists dependent on the purpose and action intended.

Use of Equipment to Monitor Noise

2.7 Where possible notification that noise will be monitored should be notified to the occupiers of the relevant property. Where this is not feasible then covert monitoring may be necessary and proportionate. The use of equipment with the intention to only monitor noise levels does not fall into the scope of Directed Surveillance and therefore no authorisation is required. This is still the case even if during the course of the monitoring snatches of conversation are inadvertently recorded, as collecting private information was not the intention of the operation. This is assuming that all that is recorded is that which can be picked up by the unaided ear. In this situation it is considered that the perpetrator has waived his right to privacy.

2.8 That said, care should be taken with equipment that has the capability of not only picking up conversation but can also attribute it to an individual. There is a risk that this could fall within the domain of intrusive surveillance, which the council is not sanctioned to authorise.

2.9 Where test purchases of age restricted items are conducted, it will not usually be necessary to seek Directed Surveillance authorisation. The exception to this is in a situation where either the juvenile undertaking the transaction or the officer observing the transaction are carrying a concealed recording device. In this instance an authorisation would be appropriate. This needs to be considered on a case by case basis and good practice dictates that a note is made of the reasoning behind the decision not to apply for a RIPA authorisation. Please refer to 7.5 which identifies where a CHIS may be required in such operations.

3. Authorisation Framework

The Authorising Officer

3.1 The Authorising Officer is one of the checks and balances built into the system to ensure that applications for covert surveillance are justified. Before authorising an application for Directed Surveillance they must be satisfied that:

a) the surveillance is necessary for the prevention or detection of serious crime

b) the surveillance is proportionate to the purpose of the operation.

3.2 An Authorising Officer should be a senior council officer (ie Head of Service or above) who has had the training and has time to meet their obligations effectively. For a list of Authorising Officers please refer to Appendix 2.

3.3 If Confidential Information is likely to be gathered as a result of Directed Surveillance, then authorisation is required from the Head or Paid Service or the person acting as Head of Paid Service in their absence.

3.4 Each service area should have a nominated Authorising Officer who will be responsible for considering all new applications as well as undertaking reviews, renewals and cancellations as appropriate.

3.5 Authorisations need to be signed with a “wet signature”. Alternatively authorising officers may use the Digital Signature facility available in MS Word to ensure the authenticity and integrity of the document. The Senior Responsible Officer (see other roles of SRO below) as well as keeping a list of all Authorising Officers will also maintain a corresponding sample “wet signature” for each Authorising Officer .

Necessity and Proportionality

3.6 Necessity and proportionality are the key tests to determine whether it is appropriate to undertake covert surveillance requiring a Directed Surveillance authorisation. It is a matter of judgement on the part of the Authorising Officer to evaluate whether the criteria of necessity and proportionality has been met. However an Authorising Officer needs to raise the bar sufficiently high to justify overriding an individual’s rights under Article 8.

3.7 There are 2 limbs to the necessity test. Firstly, the Authorising Officer needs to be clear that the purpose of the surveillance is **for preventing or detecting serious crime**. This is the only purpose for which the council is permitted to sanction covert surveillance. Please note that since November 2012 there is no longer provision for the council to use RIPA in order to investigate offences relating solely to disorder (e.g. Anti-Social behaviour). Secondly, the Authorising Officer must be satisfied that the covert surveillance is necessary for that particular case. It would be expected that other less intrusive methods had been contemplated or attempted in the first instance.

3.8 On establishing that the necessity test has been satisfied, the Authorising Officer should then go on to consider proportionality. Put very simply, this a balancing act, on the one hand considering the interests of the individual in terms of their rights to privacy against the interest of the council, who in turn are representing the wider public interest, in conducting an investigation by the most effective means available.

3.9 It is essential that the Authorising Officer articulates the decision-making process for each decision where authorisation is given. This is an important tool in the quality control process to prevent authorising becoming a mere

"rubber stamping" procedure. The council will rely on good documentation of an Authorising Officer decision to help defend against a challenge to inappropriate use of RIPA powers.

3.10 The Authorising Officer should consider the following in establishing whether an authorisation is appropriate in terms of whether the proportionality qualification is met:

a) Is the size of the operation contemplated commensurate with the seriousness of the crime.

b) Do the tactics and methods proposed minimise the intrusiveness to the subject/s of the investigation as well as any other third party (Collateral Intrusion).

c) Evidencing as far as reasonably practicable, what other methods have been considered and why they were not implemented.

d) Is this reasonable use of RIPA legislation. Are there more appropriate and less drastic means of obtaining the desired result.

3.11 Ultimately, the Authorising Officer must be comfortable and unambiguous in using the words "I am satisfied" or "I believe" in declaring that the proportionality test is met. It is not sufficient merely to make an assertion to that effect.

Collateral Intrusion

3.12 The Authorising Officer needs to safeguard and have consideration for the privacy of individuals who are not the subjects of the surveillance activity (Collateral Intrusion). As a result of the surveillance private information from such third parties is unavoidably captured.

3.13 In such a situation the Authorising Officer needs to apply the same proportionality test referred to above, to justify the surveillance. To make this judgement an application for authorisation should include an assessment of the risk of Collateral Intrusion or interference, and details of any measures taken to mitigate them.

3.14 Those carrying out the covert surveillance should inform the Authorising Officer if the investigation unexpectedly comes across any unanticipated Collateral Intrusion. In such a situation in may be necessary to cease surveillance pending consideration of a revised or new authorisation.

3.15 In the case of video or photographic evidence involving third parties, consideration can be given, subject to legal advice, to editing the material (e.g. pixilation).

Operating Environment considerations

3.16 Any person considering undertaking covert surveillance will need to be aware of particular sensitivities in the local community where the surveillance is taking place. They will also need to take account of similar activities being undertaken by other council departments or other public authorities that may impact on the proposed surveillance. Caution should be taken to ensure that the authorised activity will not be compromised by the possibility of these conflicts and it is therefore recommended that an Authorising Officer consults a senior police officer for the area in which the investigation or operation is due to take place.

Internet Investigations

3.17 Staff must consider all the normal rules and guidance applicable to any type of enquiry conducted within a criminal investigation, such as, the Data Protection Act (DPA), Criminal Procedures Investigations Act (CPIA) and RIPA when using the internet for investigations.

3.18 IPCO guidelines state that where privacy settings are available on social networking sites and not used by the individual involved, the data may be considered open source and an authorisation is not usually required. Even though such information may be open source, staff should still consider any collateral intrusion that may occur, as well as whether the use of the open source data in combination with other methods of surveillance amounts to Directed Surveillance. Additionally, repeated or systematic viewing of social media profiles or other personal information could amount to surveillance and require an authorisation.

3.19 Individuals may still have an expectation of privacy even though data is published online especially where privacy controls are used.

3.20 All staff should keep their line manager informed of the frequency and scope of their use of open source online material.

3.21 Where staff regularly use information found online, managers should ensure that all information is genuinely open source and consult the SRO if there is any doubt.

3.22 Where an investigator may need to communicate online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

3.23 Where contact is made with individuals using an account that is set up with an intention to circumvent privacy controls by deception, for example using a pseudonym to send a friend request on Facebook, a CHIS authorisation **mus**t be sought.

Best Practice – An Overview

3.24 The following principles should be adhered to with respect to all applications for authorisations covered in these procedures:

- All applications should refer to a unique reference number that is used on all forms related to that surveillance;
- Information contained in applications should be relevant and proportionate to that required by RIPA for Directed Surveillance authorisations;
- Oral authorisations are no longer available because of the new requirement for judicial approval before the commencement of an operation.
- In the instance where surveillance involved other agencies this should be noted in the authorisation;
- Where it is known that authorisation has already been granted for a particular activity either by another council department or another public authority it would not be necessary to seek authorisation.

Senior Responsible Officer

3.25 The role of Senior Responsible Officer is allocated to the Director of Law and Governance and they will be responsible for:

- Conducting quality control for all authorisations made for covert surveillance
- Maintain the central record which records significant details of each authorisation processed.
- Ensure that the processes in place to authorise Directed Surveillance are fit for purpose;
- Govern the Council's compliance with RIPA and associated Codes of Practice;
- Facilitate inspections by the Commissioner's office and where necessary, monitor the implementation of any remedial action plans suggested by the Commissioner;
- Ensure that all Authorising Officers are of an appropriate standard;
- Undertake an annual audit of records.

If at any time the Senior Responsible Officer is on leave or otherwise indisposed the Head of Regulatory Services and Corporate H&S may assume the role of SRO. The Head of Regulatory Services and Corporate H&S will be unable to act as an Authorising Officer during this time.

Role of Elected Members

3.26 Elected members of the Council are required to review the use of RIPA and to set the policy on covert surveillance at least once every 12 months. It will therefore be the responsibility of the Audit Committee to review these procedures annually and make recommendations to the Council accordingly.

3.27 The General Purposes Committee will be responsible for considering the Council's application of RIPA every 3 months (if any of the powers are used in the preceding 3-month period) to ensure that it is being used appropriately and in line with the Council's set policy and procedure.

3.28 General Purposes Audit Committee has no part in the decision-making process for individual authorisations.

Duty to Report Unauthorised Covert Activity

3.29 Any covert surveillance that is not appropriately authorised should be reported to the Chief Commissioner as soon as the oversight is identified. After initial notification by email a report detailing the circumstances and the remedial action taken should be submitted to the IPCO by the Head of Paid Service (Chief Executive) or the Senior Responsible Officer. Such a breach includes not only covert surveillance undertaken which had not been properly authorised but also where instructions mandated by the Authorising Officer were not followed. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

3.30 If it is decided to undertake covert surveillance without the protection of RIPA it is recommended that auditable documentation should be kept of any decision and actions taken. Authorising officers should regularly review the activities that are undertaken in such circumstances.

4. Confidential Information

4.1 In situations where Confidential Information is likely to be collected as a result of covert surveillance, extra care and consideration for this sensitive category of data is required. The category of Confidential Information includes material subject to legal privilege, confidential personal information (e.g. information relating to mental or physical health) or confidential journalistic material. If in any doubt as to whether information could fall into this category, officers should seek advice from Legal Services at the earliest possible opportunity.

4.2 The Applicant should complete the application for authorisation of Directed Surveillance in the normal way, accompanied with a narrative explaining the likelihood and the nature of the confidential material at risk of being gathered. However a higher level of authorisation for such surveillance is needed and therefore must be authorised by the Head of Paid Service (the Chief Executive) or, in his/her absence, acting Head of Paid Service. Such applications should only be considered in exceptional circumstances with full regard to the proportionality issues.

4.3 Confidential material must be treated with special handling at all times from its collection to the point of destruction. Any processing of it, including dissemination or storing must only be done when an appropriate officer (having sought advice from Legal Services) is satisfied that it is necessary for a specific purpose. All reasonable steps should be taken to guard against any unnecessary dissemination that could prejudice any criminal or civil proceedings related to the information. Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose. If it is retained for any purpose the Commissioners should be made aware of it so that they may be able to inspect it on request.

Confidential Information and Legal Privilege

4.4 Information that attracts legal privilege is that which is communicated between professional legal counsel and their clients where it is:

a) providing legal advice to the client; or
b) made relating to litigation or in contemplation of litigation

4.5 Communications made with the purpose of furthering criminal activity, regardless of whether the lawyer is acting knowingly or not, does not have the protection of legal privilege.

Legal Consultations

4.6 The provision of the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 requires that

Directed Surveillance takes place in a location used for the purposes of “legal consultations” shall be considered for the purposes of RIPA *as intrusive surveillance.* The Council has no powers under RIPA to authorise or carry out intrusive surveillance.

4.7 Locations identified under the 2010 Order include prisons, police stations, cells at Magistrates’ courts as well as legal chambers.

5. Procedure for obtaining Authorisation for Directed Surveillance

Overview

5.1 The council is restricted in its use of covert surveillance under RIPA and is only permitted to exercise it if it is for the purpose of **preventing or detecting serious crime**.

5.2 The nominated Authorising Officer will in addition need to take into account the proportionality and consider any potential for Collateral Intrusion.

5.3 Written authorisation using the form in annex 1 must be obtained in advance of any activities involving Directed Surveillance before it commences. All authorisation must have “wet signatures” or possess a legitimate Digital Signature (see section 3.5).

5.4 The Authorising Officer must reject any application where in their judgement the officer making the application has not provided sufficient information on which the Authorising Officer is able to make a determination on whether the covert surveillance can be legitimately undertaken. In this instance the Authorising Officer must record the reasons for this refusal on the Authorisation form and prompt the applying officer to revise the application.

5.5 In the interest of consistency and quality control, officers should make use of the relevant section of the checklist in App 3 for any Authorisation, Review, Renewal or Cancellation as appropriate.

Required Information on the Application Form

5.6 After obtaining a Unique Reference Number (URN) from the Senior Responsible Officer, the application for Directed Surveillance should be completed and include the following elements in sufficient detail:

- The need for the investigation or operation
- Why covert surveillance is justified
- Consideration of proportionality and weighing up risks and outcomes
- Surveillance methods and tactics to be deployed
- Subject of the surveillance and identities if known
- Objectives of the surveillance
- Collateral Intrusion including proportionality assessment
- Confidential Information that is likely to be acquired

Authorisation Form

5.7 On receiving the completed application (see links to sample forms in annex 1 below), the Authorising Officer should complete the relevant Authorisation section of the form. It should be noted that the information contained on the Authorisation section of the form is the only document that a court will have access to in case of a legal challenge to an authorisation to conduct Directed Surveillance. It is essential therefore that the authorisation section of the form is comprehensive and has sufficient information on it which justifies the use of the surveillance authorised. To this end the Authorising Officer should cover in some detail the *who, what, where, why and how* in any authorisation.

5.8 The Authorising Officer, after outlining the context, should explain why they *believe* and are *satisfied* that the Directed Surveillance is necessary and proportionate, if this is the case. If however the authorisation is refused, the Authorising Officer should clearly indicate this on the form and return it to the applying officer. Regardless of whether the authorisation is given or refused, copies of the completed form must be sent electronically to the Senior Responsible Officer.

Validity of Authorisations

5.9 A written authorisation for Directed Surveillance is valid for up to three months from the day on which it took effect (e.g. from 17:00 15th March to 23:59 14th June inclusive), subject to subsequent cancellation or renewal (see below).

5.10 An authorisation only takes effect once it has been granted judicial approval, not when it is authorised by the Authorising Officer.

Serious Crime Test

5.11 Authorising Officers may only authorise Directed Surveillance (this test does not apply to CHIS or Access to Communication Data applications) if it is for the purpose of preventing or detecting a criminal offence and that the offence is punishable, whether on summary conviction or on indictment, by a maximum term of **at least 6 months of imprisonment**, or 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. The latter are all offences involving sale of tobacco and alcohol to underage children.

Reviews

5.12 There is no prescribed frequency for how often reviews of authorisations should be made by the Authorising Officer and is at their discretion. However reviews must not be neglected and should be undertaken as frequently as the specific case demands. Where, for instance, the authorisation involves either Collateral Intrusion or Confidential Information or where there is a risk that the surveillance could encroach into intrusive surveillance then the reviews should be made more frequently than in other cases. Legal Services will maintain

oversight to ensure Reviews are taking place as directed on the Authorisation form.

5.13 A review would also be appropriate where proposed change in surveillance may have the impact of increasing the intrusion imposed on any individual. The Authorising Officer should be made aware of this proposed course of action so that they can consider it. If approval is given to the modified surveillance then this should be brought up at the next review to monitor their continued necessity if appropriate. A completed Renewal form (see sample form below) should be completed and returned to the Senior Responsible Officer. The Senior Responsible Officer will note the outcome of the review on the central record.

5.14 Below is an illustrated example of when a review might also be appropriate.

Example: An authorisation is originally obtained for surveillance of a second hand car dealer suspected of procuring sub-standard car components which he uses on his car stock. The authorisation includes yet unknown suppliers of the components. When an individual is subsequently identified supplying the components then it is determined that their surveillance will be beneficial to the investigation. A review might then consider turning attention to the supplier and any of his associates as well as continuing surveillance of the second hand car dealer and the authorisation will require amending to reflect this. If the investigation leads to surveillance that goes beyond the scope of the initial authorisation then it will be necessary to obtain fresh authorisation.

Renewals

5.15 An authorisation can be renewed (if necessary more than once) for a further period of three months, if the Authorising Officer considers it necessary for the authorisation to continue and the proportionality test is satisfied. The renewal form (see sample form in annex 1 below) should then be completed and sent to the Senior Responsible Officer, who will note this on the central record.

5.16 All requests for renewals should include:

- a note of when previous renewals were made;
- new information that has come to light since the original authorisation;
- necessity and proportionality considerations;
- the value of the surveillance acquired to date to the overall investigation;

Cancellations

5.17 Authorisations must be cancelled by the Authorising Officer as soon as they are satisfied that the surveillance is no longer required for their intended The form (see sample form in annex 1 below) must be completed whether the authorisation is ended before the end of its normal validity or whether the authorisation has continued to the end of its validity and has ended. The Authorising Officer should review the surveillance information (the product)

acquired and prescribe the appropriate handling as appropriate. This may be either to retain or destroy it.

5.18 The cancellation form should be completed and a copy sent to the Senior Responsible Officer. This will be recorded on the central record.

5.19 The Authorising officer should:

- Keep a record of the dates of when surveillance was undertaken as well as when the order to cease the authorisation;
- Give the reason for the cancellation;
- Ensure that any surveillance equipment is removed and returned;
- Provide directions on the management of the product;
- Ensure details of any surveillance since the last review is recorded;
- Indicate whether the objectives of the surveillance operation were met.

.

Training

5.20 All officers involved with these procedures should attend relevant training and re-fresher training to keep updated on changes in legislation and any other relevant aspects which will impact on their obligations. The Senior Responsible Officer will maintain a log of any training attended and will assist in arranging training sessions as required.

6. Central Record for Authorisations and the Senior Responsible Officer

6.1 The Senior Responsible Officer will maintain a central record of all authorisations, including the following information:

- date the authorisation was given;
- name and position of the Authorising Officer;
- unique reference number (URN) of the investigation or operation;
- title of the investigation or operation;
- Details of Judicial approval or refusal
- results of any reviews undertaken;
- if the authorisation has been renewed when and by whom;
- likelihood of acquiring “Confidential Information”;
- date that the authorisation was cancelled.

6.2 The Senior Responsible Officer will maintain this central record as and when an authorisation is granted, renewed, reviewed or cancelled. This record is required to be made available to the Inspector from the Office of the Investigatory powers Commissioners on request so it is essential that there is no delay in sending copies of all completed forms to the Senior Responsible Officer.

6.3 The central record and all the related documentation (including documentation relating to judicial approval process) is retained for three years from the date on which the authorisation expires or is cancelled.

Quality Control

6.4 As well as maintaining the central record, it is the Senior Responsible Officer’s responsibility to undertake quality checks on authorisations to ensure that the relevant procedures contained in this document and the codes of practice have been complied with. The Senior Responsible Officer will challenge any authorisations where it is shown that there are insufficient grounds of necessity or proportionality to conduct the surveillance.

Authorising Officer Case Management

6.5 The Authorising Officer should maintain the following information as part of their own record keeping:

- A copy of the application
- A signed copy of the authorisation or refusal;
- 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 outcome of each authorisation review;
- A copy of any renewal of an authorisation;
- Copy of the cancellation form

- Any supporting documentation provided either at authorisation/rejection or if applicable at renewal.

Allocation of the Unique Reference Number (URN)

6.6 The Senior Responsible Officer will provide the URN before the application is submitted to the Authorising Officer. The URN will follow a numbering convention which will denote the service that is commissioning the surveillance activity and the year that the authorisation was granted. For instance 16/EP/7/10 denotes that this is the sixteenth entry on the central record and the seventh application commissioned by Environmental Protection in 2010.

6.7 The following is a list of available codes to be used on the URNs:

CEX	**Chief Executive**
EH	**Environmental Health**
EP	**Environmental Protection**
TS	**Trading Standards**
IA	**Internal Audit**
RB	**Revenue and Benefits**
EDU	**Education**
CSU	**Community Safety Unit**

Surveillance Involving a Third Party

6.8 In the event that the police or other enforcement agency requires the use of council CCTV system, for the purposes of Directed Surveillance *they are conducting*, they must present documentation to the council authorising the operation, in the same way as if it were a council operation.

6.9 The CCTV operators must be given word for word, the precise directions given on an authorisation so that they are aware of the scope of the surveillance. This is the case whether it is a council led or third party led operation.

6.10 Similarly it is vital that the cancellation of the surveillance is immediately communicated to the CCTV operators. It is advisable where CCTV surveillance is being carried out by the council on behalf of a third party that regular checks are made with the third party to ensure that the surveillance is still required. In any event documentation must be submitted to effect the cancellation of the operation. This applies whether it is a council sponsored operation or if it is undertaken on behalf of a third party.

7. Covert Human Intelligence Sources

7.1 A person is a Covert Human Intelligence Source (or CHIS) if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating anything falling within the following:

(i) he covertly uses the relationship to obtain information or to provide access to any information to another person; or
(ii) he covertly discloses information obtained by the use of or as a consequence of such a relationship.

7.2 The difference between CHIS and Directed Surveillance is that the latter relates to acquiring private information about an individual. However a CHIS is used to covertly manipulate a relationship to obtain any information.

7.3 A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

7.4 Below are some scenarios where a CHIS is likely to be used. What is common in all of them is the establishment of a relationship that involves an element of trust:

- A source posing as a consumer at a retail outlet suspected of selling counterfeit perfume, the test purchase might involve gaining the trust of the owner, in order to find out about what items can be supplied, when and at what price.

- A source posing as a consumer at a weight loss clinic where false or misleading claims are being made to consumers

- A source posing as a customer at a night club suspected of selling methanol based spirits

7.5 Test purchases for selling of alcohol, cigarettes or knives to underage juveniles will not usually constitute a CHIS. This is because the activity is confined to the transaction surrounding the purchase (i.e. requesting, acceptance and payment). There is no gathering of information or forming of a relationship. However where such an operation is likely to elicit private information or where covert recording equipment is used then an authorisation for Directed Surveillance is appropriate. However, it may be necessary to consider authorising a CHIS in this situation if the relationship extends beyond just a single encounter.

7.6 Council officers are not permitted to engage in entrapment tactics by encouraging an individual to commit a crime that would not have committed had the tactic not been employed.

7.7 The use of informants for these purposes must be controlled and deployed within the CHIS framework. It would not be appropriate to encourage an individual to act as informal CHIS without having completed the proper assessment and authorisation.

7.8 Information from sources that is offered voluntarily to Council officers is not covered by these arrangements and do not require the authorisation of a CHIS. However such information is still subject to the provisions of the Data Protection Act 1998.

General Rules on Authorisation for CHIS

7.9 As with Directed Surveillance, CHIS will require authorisation by the nominated Authorising Officer. Similarly, authorisation must only be granted where such activity is necessary (i.e. the prevention or detection of crime) and proportionate. There must be consideration given to the potential of Collateral Intrusion.

7.10 A written authorisation for CHIS is valid for up to 12 months (except in the case of juveniles where it is 4 months). It can be renewed for a longer period provided the criteria justifying the use or conduct of the CHIS are still met. Authorising Officers should ensure that regular reviews are carried out and that the authorisation is cancelled as soon as the CHIS is no longer necessary.

7.11 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.

7.12 It is essential that the CHIS and those involved in the use of CHIS are aware of the extent and limits of any conduct authorised.

Local Considerations and Community Impact Assessments

7.13 Any person applying for or endorsing an authorisation will need to be aware of any particular sensitivities in the local community where a CHIS is operating and of any similar operations being conducted by other public authorities, which could impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may come about from the use or conduct of a CHIS or use of information obtained from that CHIS.

7.14 Where an Authorising Officer considers that a conflict might arise they should, where possible, consult with a senior Police officer in that area. The Council, where possible, should also consider conferring with other relevant public authorities to gauge community impact.

Use of CHIS with Technical Equipment

7.15 An authorised CHIS with a surveillance device does not require a separate Directed Surveillance authorisation, provided that the device will only be used in the presence of that CHIS. If the device will be used other than in the presence of the CHIS then Directed Surveillance authorisation should be obtained.

7.16 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 CHIS by the Local Authority

7.17 The requirement for elected members of the Council to review the use of RIPA every 12 months and to set the policy includes the use of CHIS (see 3.20).

7.18 Furthermore, before CHIS are authorised an overview meeting including the authorising officer, the application officer and Legal Services should take place to ensure that legal and other requirements have been considered. See the CHIS overview meeting template in Appendix 4 covering the items that should be addressed.

Management of CHIS

7.19 A structure should be in place for the managing and handling of a CHIS and an authorisation should not take place unless a CHIS can be managed effectively by ensuring:

(a) that there will at all times be someone who will have day-to-day responsibility for handling the source on behalf of the Council and is overseeing their security and welfare. This person is the handler, whose duties will include; 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 supervision of the handler and

general overview of the use of the CHIS. The controller will be senior to the handler in rank and depending on resources will normally be the Authorising Officer or equivalent in grade.

(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) the records relating to the source are maintained by the council according to Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No:2725 which details the particulars that must be included in these records.

(e) that records maintained by the authority relating to the identity of the source will not be available to persons unless there is an operational need

Security and Welfare

7.20 The Council has an obligation to consider the safety and welfare of any CHIS it deploys. Prior to authorising the use of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out, which takes into account any training and experience of that CHIS relative to the environment they will be operating in. The safety and welfare of the CHIS should continue beyond the cancellation of the authorisation. The originals should be scanned and sent electronically to Legal Services and the original should be kept by the authorising officer for their own records.

7.21 The Authoring Officer should consider using pseudonyms when referring to the authorisation of one or more undercover officer so as not to compromise their position. The Authorising Officer should be able to make a link between the pseudonym and an identifiable individual to enable them to make an individualised risk assessment.

7.22 Care should be exercised to any request for information that risks disclosing the existence or identity of the CHIS to, or in, court.

7.23 The handler should make the controller aware of any concerns about the personal circumstances of the CHIS, that might impact on:

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

7.24 Concerns about such matters must be considered by the Authorising Officer and a review on whether or not to allow the authorisation to continue.

7.25 For further information about the central record, the retention and destruction of material, the Senior Responsible Officer, see the relevant sections of these procedures.

Vulnerable Sources

7.26 The use or conduct of any source under 16 years of age living with their parents cannot be authorised to give information about their parents. Juvenile sources can give information about other members of their immediate family in exceptional cases. The authorisation should not be granted unless or until:

- The safety and welfare of the juvenile has been fully considered;
- The Authorising Officer has satisfied himself/herself that any risk has been properly explained and understood by the juvenile;
- A risk assessment has been undertaken as part of the application to deploy a juvenile source, covering the physical dangers and the moral and psychological aspects of his or her deployment.

7.27 Deployment of juvenile sources will only be authorised by the Head of Paid Service (which in the council is the Chief Executive) or in the absence of the Head of Paid Service, the Acting Head of Paid Service.

7.28 Vulnerable individuals, such as those with a mental disability, will only be authorised to act as a source in the most exceptional circumstances. Authorisation of the Head of Paid Service or in the absence of the Head of Paid Service, the Acting Head of Paid Service is required.

7.29 Sample forms associated with the CHIS process can be accessed using the links in annex 1 below.

8. Access to Communications Data

8.1 The council investigating criminal offences have powers (by virtue of the RIPA (Communications Data) Order 2004 ("the Order") to gain access to communications data – that is information held by telecommunication or postal service providers about the use of their services by person who are the subject of criminal investigations.

8.2 In using such powers, officers must have full regard to the Code of Practice on Accessing Communications Data, issued by the Home Office. As with covert surveillance access to communication data must be authorised by a designated Authorising Officer and obtained via the Single Point of Contact (SPOC).

8.3 Access to communications data is permitted only where it is necessary for the prevention or detection of crime. It needs to be proportionate to the objectives the Council is seeking to achieve i.e. it should not be authorised where less intrusive means can be used to further an investigation. The Order allows authorities to gain access to two types of communications data: -

a) Service Data
   Information held by a telecom or postal service provider about the use made of a service by a person under investigation e.g. itemised telephone bills/outgoing call data.

b) Subscriber Data
   Any other information or account details that a telecom / postal service provider holds on a person under investigation.

8.4 The council is **not** authorised to obtain access to "traffic data" i.e. information about when communications were made, who from and who to. Further these powers do not permit access to the contents of the communications itself.

8.5 There are two methods conferred by RIPA on the council to collect communications data. One permits an authorised person to permit another person in the council to collect the data. i.e. if a communications service provider is technically unable to collect the data the authorisation permits the local authority to collect the communication data itself. The second method permits the council to compel a communications service provider to disclose communications data in its possession.

8.6 Requests for communication data can only be sent by an officer who is known as a Single Point of Contact ('SPoC'). The SPoC is an officer who has undertaken the requisite training and passed an examination to achieve proper accreditation. The council utilises the SPoC service provided by the

National Anti-Fraud Network (NAFN) and the authorising officer will authorise access to Communications data applications through the NAFN service.

9. Judicial Approval

9.1 All authorisations under RIPA will require approval of a Magistrate for the use of any one of the three covert investigatory techniques available, namely Directed Surveillance, the deployment of a Covert Human Intelligence Source (CHIS) and accessing communications data.

9.2 An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. The new provisions allow the Magistrate, on refusing an approval of an authorisation, to quash that authorisation.

9.3 After the internal authorisation process is completed, the Authorising Officer will be responsible for contacting the Magistrates Court to arrange a hearing to initiate the judicial approval process.

9.4 In order for the magistrate to endorse the authorisation they must be satisfied that there are reasonable grounds for doing so and that it is both necessary and proportionate. In addition they must be satisfied that the person who granted the authorisation was an appropriate designated person within the Council and the authorisation was made in accordance with any applicable legal restrictions, for example that the serious crime threshold for directed surveillance has been met (see section on serious crime test).

9.5 Should the magistrate refuse to authorise the application the council may only appeal the decision on a point of law by making an application for judicial review in the High Court. For full details on seeking judicial approval you should refer to the Home Office guidance.

9A Access to communications Data - Judicial Approval Procedure

9A.1 The judicial approval procedure for access to communications data is slightly different. NAFN will provide the relevant officer with a Court Pack containing the following:

Final Case Application,
Judicial Application/Order form
Relevant Assurance(s), Authorisation(s) and/or Notice(s)

9A.2 These documents will enable the officer to present their application at court. If the application is subsequently approved all documentation must be returned to NAFN, where they will access their secure online systems and promptly return results.

10. Complaints

10.1 The Independent Tribunal, which consists of the judiciary and is independent of the Government, has authority to investigate complaints made to them by a individual who has a grievance in the way the powers were used by a Council under Part II of RIPA

10.2 Further information on the Tribunal and details of the relevant complaints procedure can be obtained from:

Investigatory Powers Tribunal

PO Box 33220
London
SW1H 9ZQ

020 7273 4514

10.3 The public will still have redress to the Council's internal complaints procedure, where appropriate and also to the Local Government Ombudsman.

11. The Investigatory Powers Commissioner's Office

11.1 The Investigatory Powers Commissioner's Office (IPCO) was established to regulate covert surveillance carried out by public authorities. The commissioner has powers to inspect how public authorities use their powers under RIPA.

11.2 One of the duties of the IPCO is to carry out planned inspections of those public authorities who carry out surveillance under RIPA, to ensure compliance with the statutory authorisation procedures. The inspection will examine the policies and procedures in relation to Directed Surveillance and CHIS 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.

11.3 After the inspection a report it 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.

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

11.5 There is a duty on all who use 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 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

These procedures have been produced as a guide and should be used in conjunction with the current 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.

For further information please contact the Corporate Team, Legal Services, Civic Centre, Silver Street, Enfield, EN1 3XY or call:

Terry Osborne 020 8 379 1000

Appendix 1

Sample RIPA forms

DIRECTED SURVEILLANCE

Application for Directed Surveillance Authorisation

Application for Directed Surveillance Review

Application for Directed Surveillance Cancellation

Application for Directed Surveillance Renewal

COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Application for CHIS Authorisation

Application for CHIS Review

Application for CHIS Cancellation

Application for CHIS Renewal

Appendix 2

List of Authorising Officers

Name	Role
Marion Cameron	Head of Internal Audit
Martin Rattigan	Head of Regulatory Services
Darren Woods	EPSC (CCTV) Manager

Appendix 3

Directed Surveillance Checklist

Application

1. Obtain a unique reference number (URN) from Legal Services
2. The officer applying for authorisation must complete ALL the relevant sections of the form as comprehensively as possible in order that the authorising officer has all the information available to consider the application. The essential elements include:
    a. Crime to be investigated
    b. Why covert tactic is merited
    c. What covert measures are required and why
    d. Details of who is the focus of the surveillance and who else may be affected
    e. How the surveillance is to be undertaken
3. Once appropriate sections of the form are completed the applying officer should forward the application to an Authorising Officer for authorisation.

Authorisation

4. The Authorising Officer will need to consider:
    a. Necessity
        i. Is it for the prevention or detection of serious crime
        ii. why it is necessary to use the covert techniques asked for
    b. Proportionality
        i. Balancing the scope and size of the operation against the gravity and extent of the perceived intrusion.
        ii. How and why the proposed method will afford the least intrusion possible to the target and others.
        iii. That the method to be adopted is an appropriate use of legislation and after considering the alternatives is the only reasonable option to attain the desired result.
        iv. Provide evidence of other methods considered and why they were not implemented
    c. What precisely is being authorised and specify this in the authorisation. This may not be what was applied for (i.e. the who what where when and how)

d. Duration of Authorisation must be set to the statutory period specifying the start time and date and the end time and date using 24 hour clock to avoid any confusion (e.g. authorisation to start 17:15 on 05th September 2013 and end at 23:59 on 04th November 2013). The

e. When wording the authorisation the authorising officer should consider the possibility that other individuals or vehicles may become the focus of the investigation and so avoid the need to seeking a fresh authorisation later on.

f. The authorising officer must also bear in mind not to authorise more than is deemed necessary to achieve the objectives of the operation and avoid going down the path of "just in case" . Similarly experience may dictate that several tactics need to be employed to obtain the required results.

g. The Authorising Officer should identify their rank or grade

h. Once the authorisation has been completed a copy must be passed to Legal Services for inclusion on the Central Record.

Reviews

5. The Authorising Officer should ensure Review take place as frequently as the operation demands and consider and where relevant record the following at each review:

    a. Are the proportionate and necessity criteria still being met

    b. To assess the progress of the surveillance against the stated objectives

    c. To consider whether the tactics or techniques are producing the intended results or whether alternative approach is required

    d. Can the scope of the investigation be narrowed and focused

    e. The next Review date should be sent and a copy of the completed review form should be sent to Legal Services

6. Legal Services will ensure that Reviews are undertaken as scheduled and request paperwork when this is due.

Renewals

7. Renewals must only be granted before the expiry of the authorisation and will then take effect from the date of the expiry.

8. Minor changes may be made within the renewal provided the original authorisation allowed for this. Otherwise a fresh authorisation will be necessary.

Cancellations

9. Authorising Officers where they are satisfied that they are no longer necessary should cancel the authorisation at the earliest opportunity.

10. When an authorisation expires it is still required to formally cancel the authorisation using appropriate forms.

11. The Authorising Officer should ensure the following where appropriate:

    a. Record of the dates and times surveillance took place and the order to cancel the authorisation.

    b. Record the reason for the cancellation

    c. That the equipment has been removed and returned

    d. Provide direction for the management of the product (intelligence gathered)

    e. Ensure that the details of the persons under surveillance since the last review or renewal is recorded

    f. Record of an assessment of whether the operation has met its objectives

12. On completion of the cancellation send a copy to Legal Services to add to the Central Record

Appendix 4

Covert Human Intelligence Source Overview Meeting Template

AGENDA

1. CHIS Authorisation
    a. Necessity and proportionality
    b. Use of Equipment
    c. Requirement for Directed Surveillance
2. Joint working with Police or other Authorities
3. Impact on local community of CHIS
4. Source Welfare and Management
    a. Training needs
    b. Risk Assessment
    c. Source Records
    d. Handler and Controller
5. Review (if required)

This page is intentionally left blank