RIPA Policy Document and Covert Surveillance Procedural Notes (as amended December 2019)

Summary of key changes

RIPA Policy Document

1. The Regulation of Investigatory Powers Act 2000 (RIPA) no longer governs the acquisition of communications data. This is now covered by Part 3 of the Investigatory Powers Act 2016 (IPA). However, RIPA still applies to the authorisation of the other 2 covert techniques available to the Council - (i) directed surveillance on individuals in public places and (ii) covert human intelligence sources (CHIS), where individuals interact with suspected offenders.

2. On 1 September 2017, the Investigatory Powers Commissioner's Office (IPCO) took over responsibility for oversight of investigatory powers from the Interception of Communications Commissioner's Office, the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner. Future inspections of the council's use of RIPA will be undertaken by the IPCO.

3. In August 2018, the Home Office published revised codes of practice – 'Covert Surveillance and Property Interference' and 'Covert Human Intelligence Sources'.

4. The council currently has 2 authorising officers– [redacted] The Senior Responsible Officer is [redacted] and the RIPA Co-ordinating Officer is [redacted]

5. The section in the policy document dealing with online covert activity has been updated in accordance with the revised Home Office codes of practice. New sections have also been added to the directed surveillance and CHIS procedural notes.

6. The policy document sets out that much of the information available online can be accessed without the need for RIPA authorisation. However, where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Also, if an investigation officer is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed.

Directed Surveillance Procedure Note

7. The procedure note sets out factors to be considered in establishing whether a directed surveillance authorisation is required for accessing information on a website as part of a covert investigation including:
    - Whether it is likely to result in obtaining private information about a person or group of people;
    - Whether the information is likely to provide the investigation officer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

8. There is a new section on 'general observation activities'. The general observation duties of council officers do not require authorisation under RIPA, whether covert or overt.

9. There is a new section on 'surveillance not relating to core functions'. 'Core functions' are the specific public functions undertaken by the council, in contrast to the ordinary functions which are undertaken by all public authorities e.g. employment issues and contractual arrangements. The council can only seek a RIPA authorisation in performance of its core functions.

CHIS Procedure Note

10. The procedure note provides guidance when a CHIS authorisation may be necessary. For example - where a council officer is interacting with others via the internet and the other parties could not be reasonably expected to know the officer's true identity, consideration should be given whether the activity requires a CHIS authorisation.

11. In a case where it is intended that more than one officer will share the online persona, each officer should be clearly identified in the overarching authorisation for the operation.

Obtaining Communications Procedure Note

12. The definition of communications data has changed and now falls into two categories of entity data and events data.

13. Examples of entity data include:
    - 'subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
    - information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed;
    - information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;

14. Examples of events data include:
    - information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
    - information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
    - itemised telephone call records (numbers called);

15. The procedure note includes an updated section on 'necessity'. Where the communications data sought by the council is wholly or partly events data the purpose must meet the serious crime threshold. A serious crime for the purpose of the IPA is:
    - an offence for which an adult is capable of being sentenced to one year or more in prison
    - any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal
    - any offence committed by a body corporate
    - any offence which involves, as an integral part of it, the sending of a communication
    - any offence which involves, as an integral part of it, a breach of a person's privacy

16. Authorisations for the obtaining of communications were previously approved by a Magistrate. The procedure note sets out the changes introduced by the IPA and the arrangements for authorisation by officers at the Office for Communications Data Authorisations (OCDA).

17. The council is still required to use the single point of contact (SPoC) at the National Anti-Fraud Network (NAFN) to facilitate the acquisition of communications data from the telecommunications and postal operators. The SPoC now also has a role in liaising between the council and OCDA.

18. The council can't make an application for communications data that requires the processing or disclosure of internet connection records for any purpose. This important exception is highlighted in the procedure note.

19. The Senior Responsible Officer for the obtaining of communications data is [redacted]

Marina Lipscomb

December 2019

ISLINGTON

RIPA POLICY DOCUMENT AND COVERT SURVEILLANCE PROCEDURAL NOTES

1. LBI RIPA POLICY DOCUMENT

2. LBI COVERT SURVEILLANCE PROCEDURAL NOTES

- Directed Surveillance
- Covert Human Intelligence Sources
- Obtaining Communications Data

3. APPENDICES

December 2019

POLICY DOCUMENT AND PROCEDURAL NOTES FOR RIPA 2000

INDEX

Section 1

LONDON BOROUGH OF ISLINGTON

POLICY FOR RIPA 2000

Introduction

1. The purpose of this policy document and the following procedural notes is to provide clear guidance on how covert surveillance can be undertaken by the Council. The documents set out the legal background and the processes for obtaining authorisation to undertake covert surveillance.

2. The Regulation of Investigatory Powers Act 2000 ("RIPA") creates a regulatory framework to govern the way public authorities handle and conduct covert investigations. A copy of RIPA can be downloaded from the HMSO website at **www.hmso.gov.uk**. The relevant codes of practice can be downloaded from the Home Office website and relevant links are set out below at paragraph 8.

3. RIPA allows local authorities to authorise the use of 2 covert techniques:
   (i) directed surveillance on individuals in public places; and
   (ii) covert human intelligence sources (CHIS), where individuals interact with suspected offenders.

Compliance with ECHR

4. RIPA was introduced to ensure that covert surveillance carried out by public authorities complies with the European Convention on Human Rights ("ECHR"). Some of these rights are absolute (such as the prohibition on torture) while others are qualified meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied.

5. Amongst the qualified rights is a person's right to respect for their private and family life as provided by Article 8 of the ECHR. Article 8 is most likely to be engaged when public authorities seek to obtain private information about a person by means of covert surveillance.

6. Article 8 of the European Convention on Human Rights ("ECHR") provides:

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The Investigatory Powers Commissioner's Office ("IPCO")

7. On 1 September 2017, the Investigatory Powers Commissioner's Office (IPCO) took over responsibility for oversight of investigatory powers from the Interception of Communications Commissioner's Office, the Office of Surveillance Commissioners ("OSC") and the Intelligence Services Commissioner. Future inspections of the council's use of RIPA will be undertaken by the IPCO; previous inspections were carried out by the OSC. In December 2014 the OSC published an updated procedures and guidance document. This document was prepared in response to frequent requests for guidance from public authorities and also sets out matters raised or identified during inspections. In the absence of case law, the opinions expressed by the Surveillance Commissioners are the most reliable indicators of likely judicial interpretation. Applicants and authorising officers should take note of the document when preparing and authorising applications for the use of covert surveillance.

Codes of Practice

8. RIPA provides that all codes of practice relating to the Act are admissible as evidence in criminal and civil proceedings. In August 2018 the Home Office published revised codes of practice – 'Covert Surveillance and Property Interference' and 'Covert Human Intelligence Sources'. The codes are available at

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

Investigation and authorising officers should refer to the relevant code of practice when constructing and considering applications.

Authorisation process

9. An application to undertake directed surveillance or to use a CHIS must firstly be authorised internally. The authorising officer must be a Director, Head of Service, Service Manager or equivalent and a list of the council's authorising officers is available on Izzi. Only the [redacted] may authorise changes to this list. It is intended that the number of authorising officers in Islington will be limited to 12.

10. However, if the investigation or operation involves confidential information, the authorisation should be given by the Head of Paid Service (the Chief Executive) or in his/her absence a Corporate Director. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

11. The authorisation must then be approved by a magistrate – a District Judge or JP.

Admissibility of evidence

12. A court may rule evidence obtained without a RIPA authorisation to be inadmissible. It is advisable, therefore, to ensure that RIPA is complied with at all times. Even if a breach does not result in evidence being excluded, there may be a finding that the Council has breached an individual's human rights. This could lead to a claim for compensation or complaints to the Local Government Ombudsman or referral to a RIPA tribunal.

Islington Council's Central Register

13. All investigation officers seeking RIPA authorisation must contact Legal Services for a Unique Reference Number ("URN") at RIPA@islington.gov.uk

14. All RIPA applications for authorisation, renewal forms (if any), review forms and cancellation forms must be marked with the allocated URN.

15. The central register is held by Legal Services. This is a central record of all RIPA authorisations and is regularly updated whenever an authorisation is approved, renewed or cancelled. Where an application for RIPA authorisation is not approved this is also recorded on the central register. The central register will be made available to an inspector from IPCO, upon request.

16. At each stage of the authorisation process the investigating officer should send an update to Legal Services with a copy of the relevant form to RIPA@islington.gov.uk. The following information is recorded on the central register:

- URN of the investigation or operation;
- Title of the investigation or operation, including a brief description and names of subjects, if known;
- Type of authorisation;
- Name and rank/grade of the authorising officer;
- Date the authorisation was given;
- Whether the investigation or operation is likely to result in obtaining confidential information;
- Whether the authorisation was granted by an individual directly involved in the investigation;
- Date the Magistrate grants approval;
- Date the surveillance commenced;
- Review dates;
- If the authorisation is renewed – name and rank/grade of the authorising officer and date when it was authorised internally and by a Magistrate;

- Date the surveillance ceased;
- Date the authorisation was cancelled.

17. The investigating officer should send copies of the following documents to Legal Services to be held as part of the central register:

- RIPA application form with record of internal authorisation;
- Application for Magistrates' approval and order granting approval (including date of attendance at court, the determining magistrate, the decision of the court and the time and date of that decision);
- Record of the results of each review;
- Renewal application with record of internal authorisation and Magistrate's order granting approval.

Online covert activity

18. The growth of the internet, and the extent of the information that is now available online, presents new opportunities for investigation officers to view or gather information which may assist the Council in preventing or detecting crime.

19. Much of the information available online can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation will not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded, RIPA authorisations may need to be considered.

20. The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. If an investigation officer is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed.

Internal monitoring

21. The Council appoints its Senior Responsible Officer ("SRO") from the Corporate Management Board. The SRO is responsible for overseeing:

- the integrity of the council's authorisation process
- compliance with RIPA and the codes of practice
- co-ordinating inspections by the IPCO
- implementation of any post-inspection action plans recommended by an inspector
- that all authorising officers meet the required standards set by the codes of practice

26. The current SRO is the [redacted]. The SRO holds 6 monthly meetings with Legal Services to review the central register and audit the quality of authorisations that have been approved in the previous 6 months.

27. Councillors have a formal scrutiny role in relation to RIPA and 6 monthly reports are submitted to Members.

28. The current RIPA Co-ordinating Officer is [redacted] The RIPA Co-ordinating Officer is responsible for:

- Reviewing the RIPA policy document and procedural notes
- Arranging training and updates for investigating officers and authorising officers
- Issuing URNs for RIPA authorisations
- Maintaining the Central Register of RIPA authorisations
- Preparing agendas and minutes for the review meetings with the SRO

Section 2.1

LONDON BOROUGH OF ISLINGTON

PROCEDURAL NOTES FOR RIPA 2000

DIRECTED SURVEILLANCE

INDEX

2.1 Directed Surveillance

2.1.1 When can the Council carry out directed surveillance?

The Council can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco.

The Council cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable by a maximum term of at least 6 months' imprisonment.

2.1.2 Who are the authorising officers?

The level of Officer who may authorise directed surveillance needs to be determined in accordance with the Regulations made by the Secretary of State. In local authorities, this is restricted to Directors, Heads of Service, Service Managers or equivalent.

The Council currently has 2 authorising officers:-

- [redacted]
- [redacted]

The list of named officers who can authorise RIPA requests is maintained on the Council's Intranet (Izzi). However, if the investigation or operation involves confidential information, the authorisation should be given by the **Head of Paid Service** (the Chief Executive) or in his or her absence a Corporate Director.

Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

2.1.3 Surveillance

Surveillance includes:

- monitoring, observing, listening to persons, their movements, conversations, other activities or communications
- recording anything monitored, observed or listened to in the course of surveillance
- surveillance, by or with, assistance of a surveillance device

By section 26(9)(2) of the 2000 Act, surveillance is covert surveillance if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

RIPA provides for 2 types of surveillance:-

a. Directed surveillance (that will be considered in more detail in this chapter) and
b. Intrusive surveillance.

Intrusive surveillance is, broadly speaking, covert surveillance carried out in relation to anything taking place on any residential premises or private vehicle and involving the presence of an individual on the premises or in the vehicle or carried out by a surveillance device. If the surveillance device is not on the premises or in the vehicle it is not considered to be intrusive, unless it consistently provides information of the same quality as if it was on the premises or in the vehicle. **This type of surveillance goes beyond the powers of local authority investigators** but the Council can approach the police to ask them to undertake such surveillance where it can be shown to be justified. In such cases, it would be for the police to seek appropriate authorisations.

2.1.4 Directed surveillance

Directed surveillance is defined in section 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and undertaken:

a) For the purposes of a specific investigation or specific 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 the 2000 Act to be sought for the carrying out of the surveillance.

The general observation duties of enforcement officers do not require authorisation under RIPA, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people.

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, an enforcement officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of a patrol.

2.1.5 Private information

RIPA defines 'private information' as any information relating to a person's private or family life. This will include any aspect of a person's private or personal relationship with others including family and professional or business relationships.

Although a person may have 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.

Example: The Council has intelligence that a number of youths that are suspected of gang activity on an estate often congregate in a local café. Although the youths are associating in a public place they will have a reasonable expectation of privacy over the contents of their conversation. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for the Council to record or listen to the conversation as part of a specific investigation.

See further examples at paragraphs 3.3 – 3.6 of the Home Office Revised Code of Practice 'Covert Surveillance and Property Interference'.

2.1.6 Online covert activity

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by the Council of that information. Also individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where an investigation

officer is proposing to systematically collect and record information about a particular person or group, a directed surveillance authorisation should be considered.

In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide the investigation officer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

See examples at paragraphs 3.15 and 3.17 of the Home Office Revised Code of Practice 'Covert Surveillance and Property Interference'.

2.1.7 General observation activities

The general observation duties of Council officers do not require authorisation under RIPA, whether covert or overt. Such general observation duties do not include pre-planned surveillance of a specific person or group of people.

General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation.

Example: Trading Standard 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 and their intention is, through reactive enforcement action, to identify and tackle offenders. This is part of the general duties of the council and the obtaining of private information is unlikely. A directed surveillance authorisation is therefore not required.

See further examples at paragraph 3.33 of the Home Office Revised Code of Practice 'Covert Surveillance and Property Interference'.

2.1.8 Surveillance not relating to core functions

'Core functions' are the specific public functions undertaken by the Council, in contrast to the ordinary functions which are undertaken by all public authorities e.g. employment issues and contractual arrangements. The Council can only seek a RIPA authorisation in performance of its core functions.

See examples at paragraph 3.35 of the Home Office Revised Code of Practice 'Covert Surveillance and Property Interference'.

2.1.9 Necessity

The authorising officer must believe that the activities to be authorised are necessary for the prevention or detection of crime.

In order to be necessary the proposed surveillance must be needed to achieve a certain desired effect or result.

What are the aims and objectives of the investigation? If you cannot state what is intended to be achieved as a result of an investigation, then it cannot be shown that the proposed surveillance is necessary as part of the process to achieve those aims and objectives.

Will gaining of the information by means of the directed surveillance, benefit the investigation? If there is no benefit, then there is no necessity.

2.1.10 Proportionality

If the activities are deemed necessary, the authorising officer must also believe that they are proportionate to what is sought to be achieved by carrying them out. No activity should be considered proportionate if the information sought could reasonably be obtained by other less intrusive means. If alternative means exist, then the authorising officer will need to consider why those alternative means should not be used over directed surveillance. If this cannot be shown, then the investigating officer will be unable to demonstrate proportionality.

In order to be proportionate, the proposed surveillance must not be arbitrary, unfair or excessive. Proportionality is about balancing the seriousness of the crime or the wrong-doing being investigated and the threat to the general public against the interference with the privacy of the individual concerned and the risk of collateral intrusion.

The following elements of proportionality should be considered:

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

- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;

- evidencing, as far as reasonably practicable, what other methods have been considered and why they have not been implemented, or implemented successfully.

The considerations as to whether an action is proportionate and whether any action is necessary do overlap, however each still needs to be considered separately, as whilst an action may be necessary it may not be proportionate.

The RIPA application should be presented in a fair and balanced way. In particular, information which weakens the case for the authorisation should be taken into account.

2.1.11 Collateral intrusion

Collateral intrusion is the risk of obtaining private information about persons who are not subjects of the surveillance.

Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity.

Where collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion is considered proportionate to what is sought to be achieved.

All applications should include an assessment of the risk of collateral intrusion and the measures to limit this. If an automated system such as an online search engine is used to obtain the information, the authorisation request should identify its potential extent and limitations.

Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes, subject to appropriate data protection safeguards in terms of handling, retention and destruction.

Where an investigation officer intends to access a social media or other online account to which they have been given access with the consent of the owner, the officer will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered.

See examples at paragraphs 4.13, 4.15 and 4.16 of the Home Office Revised Code of Practice 'Covert Surveillance and Property Interference'.

2.1.12 Combined authorisations

A single authorisation may combine 2 or more different authorisations for directed surveillance or a CHIS. However, where an officer seeks separate authorisations, consideration should be given to whether reference to these in the related authorisations is appropriate.

2.1.13 Use of Private Investigators

The Council on occasions instructs private investigators ("PI") to undertake directed surveillance. The officer in the case wishing to instruct a PI should follow the procedure set out below:-

(i) The officer should mention the use of the PI in the application for authorisation.

(ii) In the letter of instruction the PI should be made aware of the parameters of the surveillance activity.

(iii) The PI should be instructed to handover all surveillance material obtained.

(iv) The officer should check with the PI at the conclusion of the surveillance that all surveillance material has been handed over to the Council.

Any contract with a PI should be subject to binding commitments to observe council policies and data protection legislation. Where, there is a controller-processor relationship, the contract engaging the PI should observe the requirements of Article 28 of the GDPR.

2.1.14 Tracking devices

The use of a tracking device for the purpose of providing information about the location of any private vehicle may be authorised as directed surveillance. However, a property interference authorisation may be appropriate for the covert installation or deployment of the device. The Council cannot obtain a property interference authorisation and if this is required the investigating officer will have to approach the police to obtain the necessary authorisation.

2.1.15 Authorisation of directed surveillance

Authorisation will provide lawful authority for a public authority to carry out directed surveillance.

The code of practice and guidance from the IPCO should be consulted by the investigating officer when completing the application form and by the authorising officer when deciding whether to authorise the proposed surveillance.

It is important to note that only the conduct and activities specified and described in the authorisation can be carried out as part of the directed surveillance.

Authorising officers should not normally be responsible for authorising operations in which they are directly involved.

The authorisation must be approved by a Magistrate before it can take effect. Following the implementation of the Protection of Freedoms Act 2012 officers will need to satisfy the Magistrate that the following five conditions are met before an application for approval will be granted:

1) at the time of the grant of authorisation there were reasonable grounds for believing the covert surveillance authorisation was necessary and proportionate
2) at the time when the Magistrate is considering the matter, there remains reasonable grounds for believing the requirements are met
3) the officer making the authorisation was of the correct office/rank
4) the authorisation was not in breach of any restriction imposed by the Secretary of State pursuant to s30(3)
5) any other conditions imposed by the Secretary of State have been complied with e.g. as set out in any notice or statutory instrument.

2.1.16 Completing the authorisation form

Relevant authorisation forms can be found at www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/. Forms must be used for requesting a RIPA application and reviewing, cancelling or renewing it.

All investigation officers seeking RIPA authorisation must contact Legal Services for a Unique Reference Number ("URN") at RIPA@islington.gov.uk All RIPA authorisation forms must be marked with the allocated URN.

The authorisation form should include the following information without exception:-

1. State the name and position (i.e. job title) of the authorising officer.

2. Describe the conduct to be authorised (i.e. what is being done) and the purpose of the investigation or operation (i.e. obtaining evidence to consider whether a specific crime is being or has been committed). The anticipated length of time of the surveillance should be specified

3. Explain why the directed surveillance is necessary for the purpose of preventing or detecting crime and in this context:
   (a) Specify the crime or wrong being investigated (i.e. name the offence including statute and sections) and the sentence duration;
   (b) Set out the aims and objectives for which the surveillance is to be undertaken; and
   (c) Explain how the gaining of information from the directed surveillance will benefit the investigation.

4. Explain why the directed surveillance is proportionate to what it seeks to achieve and in this context:
   (a) Ensure that the objectives of the surveillance are properly defined;
   (b) Explain why the surveillance will achieve those objectives;
   (c) Specify why the surveillance should be used in preference to other, less intrusive methods of investigation; and
   (d) Specify why it would also be more practicable to use surveillance over less intrusive methods of investigation.

5. Describe the nature of the surveillance to be authorised and in this context:
   (a) Set out the location of the person who is the subject of the surveillance or where such surveillance is to take place including details of any vehicle or premises involved;
   (b) Describe the type of surveillance device or equipment to be used;
   (c) Give details of name(s) (where known) or description(s) of the person(s) who is/are to be the subject of the surveillance as well as any known history and character of that/those person(s).

6. Give an explanation of the information that it is desired to be obtained as a result of the directed surveillance (i.e. the end product).

7. Consider collateral intrusion and set out the risk of information relating to third parties' (i.e. persons not part of the investigation) private and family life being obtained. Again, this assessment must satisfy the test of proportionality. An example of collateral intrusion is the recording of a test purchase where activities (including conversations) of other customers within the premises may be captured.

8. Advising as to the likelihood of acquiring confidential information.

9. Setting out the anticipated start of the directed surveillance: both time and date.

10. Setting out the name and other relevant details of the applicant. This is also where the applicant will sign.

11. The authorising officer must comment as to why s/he considers that the directed surveillance is both necessary and proportionate. The authorising officer cannot just specify 'see above' but can paraphrase what has been stated earlier providing, of course, that they agree with those comments.

12. The authorising officer must make an independent decision and be in a position to justify the decision if necessary. The authorising officer formally authorises the surveillance and must include a date on which s/he will review the authorisation if the surveillance is still ongoing.

2.1.17 Seeking approval from a Magistrate

The authorisation form together with two copies of the application for judicial approval and a partially completed court order form should be taken to the court. The Court Office legal advisor will check the application paperwork and advise the officer which court room the application will be heard in. There is no fee, at present, for this application. The officer presenting the case at court does not need to be a lawyer, but should be the investigating officer or authorising officer

with detailed understanding of the case and have the relevant delegated authorisation to appear before the Court.

At Court, the Magistrate may not be familiar with the RIPA requirements. The officer should check with the Magistrate if they would like to be taken through the application. The Magistrate may not require this but they will generally appreciate the offer.

When taking them through the application, or the entire authorisation, the officer should explain:

- The purpose of the application
- The covert technique being sought
- The criminal offence being investigated and sentence duration
- The background to the application
- The date and officer who granted the initial authorisation

The Court Clerk may also ask questions of the officer.

2.1.18 How long does an authorisation last?

An authorisation for directed surveillance will last for 3 months. If the directed surveillance is concluded within those 3 months then the authorisation must be cancelled with immediate effect. The authorisation cannot just be allowed to lapse. The investigating officer must complete a cancellation form to be signed off by the authorising officer. The cancellation form must be marked with the allocated URN.

Before the expiry of 3 months, if the officer has not completed the directed surveillance and considers that it will go beyond 3 months then the officer must apply for the renewal of the directed surveillance to enable it to continue beyond the 3 months. A renewal form must be completed and submitted to the authorising officer and the Magistrate for approval for the directed surveillance to continue. The officer is required to give to the authorising officer and thereafter the Magistrate the following information:

- whether it is the first or subsequent renewal;

- detail(s) of any significant changes to the information as listed in the original authorisation;
- detail the reasons why it is necessary to continue with the surveillance;
- detail why the directed surveillance is still proportionate;
- indicate the content and value to the investigation of the information so far obtained;
- give details of the regular reviews (see below); and
- a copy of the original authorisation.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but investigation officers must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a Magistrate to consider the application). The renewal form must be marked with the allocated URN.

2.1.19 Reviewing an authorisation

When authorising the surveillance or granting a renewal, the authorising officer is required to set a date for review. Regular reviews should be undertaken by the authorising officer to assess the need for the surveillance to continue. On review the authorising officer will consider if the authorisation is still necessary on the ground under which it was granted or renewed and if it is still proportionate to what is sought to be achieved by carrying it out. The authorising officer must complete a review form.

The review is the responsibility of the original authorising officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms.

If after the first review the authorising officer considers that the directed surveillance is to continue then s/he will be required to set a further date of review.

All forms should be sent to the RIPA Co-ordinating Officer at RIPA@islington.gov.uk to be held in the Central Register.

2.1.20 Urgent authorisations

The Council cannot orally authorise the use of RIPA techniques. All authorisations must be in writing and require a Magistrate's approval.

A case will be urgent where, in the judgement of the investigating officer, delay will be likely to jeopardise the investigation or operation. An authorisation is not to be treated as urgent where the officer who wished to seek authorisation neglected to make the application diligently and in time.

If out of hours' access to a Magistrate is required then the officer should contact Legal Services as soon as possible so that arrangements can be made with Highbury Corner Magistrates' Court. The officer will need to provide two partially completed judicial application/order forms so that one can be retained by the Magistrate. The officer should provide the court with a copy of the signed judicial application/order form the next working day.

In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior Magistrate approval.

No RIPA authority is 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 an officer conceals himself to observe what is happening).

2.1.21 Cancellations

As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s) as soon as reasonably practicable.

The date the authorisation is cancelled will be recorded in the central register and documents directing the surveillance to cease should be retained.

2.1.22 The central register

The central register is held by Legal Services. This is a central record of all RIPA authorisations and is regularly updated whenever an authorisation is approved, renewed or cancelled. Where an application for RIPA authorisation is not approved this is also recorded on the central register.

At each stage of the authorisation process the investigating officer should send an update to Legal Services with a copy of the relevant form to RIPA@islington.gov.uk. Details of the information recorded on the central register and copies of the documents that should be sent to Legal Services to be held as part of the central register are set out at paragraphs 16 -17 of LBI's RIPA Policy Document.

2.1.23 Other records to be maintained by the Council

The relevant Council department should also keep records of the following documentation which will not form part of the central register:

- a record of the period over which the surveillance has taken place;
- the date and time of when instruction was given for the surveillance to cease;
- the date and time when any instruction was given by the authorising officer.

Section 2.2

LONDON BOROUGH OF ISLINGTON

PROCEDURAL NOTES FOR RIPA 2000

COVERT HUMAN INTELLIGENCE SOURCES

INDEX

2.2 Covert Human Intelligence Source

2.2.1 Definition of a covert human intelligence source ("CHIS")

Under RIPA a person is a CHIS if:-

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

(b) they covertly use such a relationship to obtain information or to provide access to any information to another person; or

(c) they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

2.2.2 Scope of 'use' or 'conduct' authorisations

An authorisation may be obtained under RIPA for the use or conduct of a CHIS.

The use of a CHIS involves any action on behalf of the Council to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS. In general, an authorisation for use of a CHIS will be necessary to authorise steps taken by the Council in relation to a CHIS.

The authorisation for conduct of a CHIS will authorise steps taken by the CHIS on behalf, or at the request, of the Council.

Most CHIS authorisations will be for both use and conduct of a CHIS. The CHIS must be clear what is/is not authorised and all the CHIS's activities should be properly risk assessed.

2.2.3 Identifying when a human source becomes a CHIS

Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer who discloses information out of professional or statutory duty, or has been tasked to obtain information other than by way of a relationship.

Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to a public authority on a repeated basis and need to be managed appropriately to establish whether, at any given stage, they should be authorised as a CHIS.

See examples at paragraphs 2.18, 2.23 and 2.25 of the Home Office Revised Code of Practice 'Covert Human Intelligence Sources'.

2.2.4 Necessity and proportionality

The authorising officer must believe that the activities to be authorised are necessary for preventing or detecting crime or preventing disorder.

If the use or conduct of the CHIS is deemed necessary, the authorising officer must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the seriousness of the intrusion into the private or family life of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation;
- whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

2.2.5 Extent of authorisation

An authorisation for the use or conduct of a CHIS will provide lawful authority for any 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.

The CHIS, and the officers involved in the use of the CHIS, must be fully aware of the extent and limits of any conduct authorised.

2.2.6 Collateral intrusion

Collateral intrusion is the risk of obtaining private information about persons who are not subjects of the surveillance. Before authorising the use or conduct of a CHIS, the authorising officer should take into account the risk of interference

with the private and family life of persons who are not the intended subjects of the CHIS activity.

Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity.

Where collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion is considered proportionate to what is sought to be achieved.

All applications should include an assessment of the risk of collateral intrusion and the measures to limit this.

Where CHIS activity is deliberately proposed against individuals who are not suspected of direct or culpable involvement in the matter being investigated, interference with the private or family life of such individuals should be considered as intended intrusion. Any such interference should be carefully considered against the necessity and proportionality criteria as described above.

See examples at paragraph 3.12 of the Home Office Revised Code of Practice 'Covert Human Intelligence Sources'.

2.2.7 Online covert activity

An officer of the Council can use the internet to interact with others, whether by publicly open websites such as a social networking service, or by more private exchanges such as, e-messaging sites. In circumstances where the other party could not reasonably be expected to know the officer's true identity, consideration should be given whether the activity requires a CHIS authorisation. A directed surveillance authorisation should also be considered unless the acquisition of that information will be covered by the CHIS application.

A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Where a Council officer sets up a false identity to register on a site, this does not of itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information.

Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request, this may not amount to establishing a relationship. However, this may lead to further interaction where a CHIS authorisation is required.

Where it is intended that more than one officer will share the online persona, each officer should be clearly identified in the overarching authorisation for the operation.

See examples at paragraphs 4.13 and 4.14 of the Home Office Revised Code of Practice 'Covert Human Intelligence Sources'.

2.2.8 Authorisation of covert human intelligence sources

Authorisation will provide lawful authority for a public authority for the use or conduct of a CHIS.

The code of practice and guidance from the IPCO should be consulted by the investigating officer when completing the application form and by the authorising officer when deciding whether to authorise the proposed surveillance.

It is important to note that only the conduct and activities specified and described in the authorisation can be carried out as part of the covert surveillance. All the CHIS's activities should be properly risk assessed.

A 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 the CHIS.

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 their presence.

The authorisation must be approved by a Magistrate before it can take effect.

Following the implementation of the Protection of Freedoms Act 2012 officers will need to satisfy the Magistrate that the following five conditions are met before an application for approval will be granted:

1) At the time of the grant of authorisation there were reasonable grounds for believing the covert surveillance authorisation was necessary and proportionate
2) At the time when the Magistrate is considering the matter, there are still reasonable grounds for believing the requirements are met
3) The officer making the authorisation was of the correct office/rank
4) The authorisation was not in breach of any restriction imposed by the Secretary of State pursuant to s30(3)
5) Any other conditions imposed by the Secretary of State have been complied with e.g. as set out in any notice or statutory instrument.

If the Magistrate is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate they will issue an order approving the authorisation.

2.2.9 <u>What information should be contained in the authorisation forms?</u>

Relevant authorisation forms can be found at

https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwi36KyBI-

Forms must be used for requesting authorisation and reviewing, cancelling or renewing it.

All investigation officers seeking RIPA authorisation must contact Legal Services for a Unique Reference Number ("URN") at RIPA@islington.gov.uk All RIPA authorisation forms must be marked with the allocated URN.

The application for authorisation should include the following information:

- The reason why the authorisation is necessary i.e. to detect/prevent crime or detect disorder
- The purpose for which the CHIS will be tasked or deployed
- Where a specific investigation or operation is involved, the nature of that investigation or operation
- The nature of what the CHIS conduct will be
- 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 authorisation
- The reasons why the authorisation is considered proportionate to what it seeks to achieve
- A record of whether authorisation was given or refused, by whom and the time and date

2.2.10 Seeking approval from a Magistrate

The authorisation form together with two copies of the application for judicial approval and a partially completed court order form should be taken to the court. The Court Office legal advisor will check the application paperwork and advise the officer which court room the application will be heard in. There is no fee, at present, for this application. The officer presenting the case at court does not need to be a lawyer, but should be the investigating officer or authorising officer

with detailed understanding of the case and have the relevant delegated authorisation to appear before the Court.

At Court, the Magistrate may not be familiar with the RIPA requirements. The officer should check with the Magistrate if they would like to be taken through the application. The Magistrate may not require this but they will generally appreciate the offer. When taking them through the application, or the entire authorisation, the officer should explain

- The purpose of the application
- The covert technique being sought
- The criminal offence/disorder being investigated
- The background to the application
- The arrangements in place to manage the CHIS
- The date and officer who granted the initial authorisation.

The Court Clerk may also ask questions of the officer.

2.2.11 How long does an authorisation last?

An authorisation for use or conduct of a CHIS will last for 12 months.

The authorising officer must cancel the authorisation if they are satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation. The investigating officer must complete a cancellation form to be signed off by the authorising officer. The cancellation form must be marked with the allocated URN.

Before the expiry of 12 months, if the officer has not completed the directed surveillance and considers that it will go beyond 12 months then the officer must apply for the renewal of the CHIS. A renewal form is required to be completed and submitted to the authorising officer and the Magistrate for approval for the conduct of the CHIS to continue.

Before an authorising officer renews an application, they must be satisfied that a review has been carried out of the use of a CHIS, as outlined below, and that the results of the review have been considered.

The officer is required to give to the authorising officer and thereafter the Magistrate the following information

- Whether it is the first renewal or every occasion on which the authorisation has been reviewed previously
- Any significant changes to the information in the initial application
- The reasons why it is necessary for the authorisation to continue
- The use made of the CHIS
- The tasks given to the CHIS and the information obtained from the use or conduct of the CHIS
- The results of the regular reviews of the use of the CHIS.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but investigation officers must take account of factors that may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a Magistrate to consider the application). The renewal form must be marked with the allocated URN.

2.2.12 Review of an authorisation

Regular reviews of authorisations should be undertaken by the authorising officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified. The review should include the use made of the CHIS during the period authorised, the tasks given to the CHIS and the information obtained from the CHIS. There should be frequent reviews of authorisations where the use of a CHIS provides access to confidential information or involves significant collateral intrusion.

The authorising officer will decide how often a review should take place. This should be as frequently as is considered necessary and practicable, but should not prevent reviews being conducted in response to changing circumstances.

2.2.13 Urgent authorisations

Local authorities cannot orally authorise the use of RIPA techniques. All authorisations must be in writing and require a Magistrate's approval.

A case will be urgent where, in the judgement of the authority officer, delay will be likely to jeopardise the investigation or operation. An authorisation is not to be treated as urgent where it is down to the officer who wished to seek authorisation failed to make the application diligently.

If out of hours access to a Magistrate is required then the officer should contact Legal Services as soon as possible so that arrangements can be made with Highbury Corner Magistrates' Court. The officer will need to provide two partially completed judicial application/order forms so that one can be retained by the Magistrate. The officer should provide the court with a copy of the signed judicial application/order form the next working day.

In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior Magistrate approval.

2.2.14 Management of covert human intelligence sources

Tasking

Tasking is the assignment given to the CHIS. The RIPA authorisation should cover the nature of the source's task. This should be in reasonably broad terms - authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If there is a step change in the

nature of the task that significantly alters the entire deployment, then a new authorisation may need to be sought.

It may be difficult to predict exactly what might occur when the CHIS meets the subject of an investigation. If there is an unforeseen occurrence this must be recorded as soon as practicable and it should be referred to the authorising officer. The authorising officer will consider if the existing authorisation is sufficient or if it needs to be cancelled and replaced.

Handlers and controllers

The handler will have day-to-day responsibility for

- Dealing with the CHIS on behalf of the Council
- Directing the day-to-day activities of the CHIS
- Recording the information supplied by the CHIS
- Monitoring the CHIS's security and welfare

The handler will usually be of a rank or position below that of the authorising officer.
The controller will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

Security and welfare

Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known.

The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Consideration should also be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, court.

The handler is responsible for bringing to the attention of the controller any concerns about the personal circumstances of the CHIS insofar that they might affect the risk assessment and the safety and welfare of the CHIS. If necessary, the authorising officer will need to consider if the authorisation should be allowed to continue.

2.2.15 The central register

The central register is held by Legal Services. This is a central record of all RIPA authorisations and is regularly updated whenever an authorisation is approved, renewed or cancelled. Where an application for RIPA authorisation is not approved this is also recorded on the central register.

At each stage of the authorisation process the investigating officer should send an update to Legal Services with a copy of the relevant form to RIPA@islington.gov.uk. Details of the information recorded on the central register and copies of the documents that should be sent to Legal Services to be held as part of the central register are set out in LBI's RIPA Policy Document. These records should be retained for a period of at least five years.

2.2.16 Other records to be maintained by the Council

The relevant Council department must keep detailed records of the authorisation and use made of a CHIS. The authorising officer must not grant an authorisation for use of a CHIS unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS.

The relevant council department should also keep records of the following documentation which will not form part of the central register for at least 5 years:

- Any risk assessment made in relation to the CHIS
- The circumstances in which tasks were given to the CHIS
- The value of the CHIS to the authority

- The date and time when any instruction was given by the authorising officer that the conduct or use of the CHIS must cease

The records should preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by the CHIS.

2.2.17 Juveniles and vulnerable adults

Although a CHIS can be either a juvenile or a vulnerable adult, the Council's policy is that such persons will not be used as CHIS.

Section 2.3

LONDON BOROUGH OF ISLINGTON

PROCEDURAL NOTES FOR RIPA 2000

OBTAINING COMMUNICATIONS DATA

INDEX

2.3.1 What is communications data?

Communications data embraces the 'who', 'when', 'where' and 'how' of a communication but not its content (what was said or written).

Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services i.e. postal services or telecommunications services. All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories of entity data and events data.

Examples of entity data include:

- 'subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";

- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;

- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;

- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and

- information about selection of preferential numbers or discount calls.

Examples of events data include, but are not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);

- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;

- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);

- itemised telephone call records (numbers called);

- itemised timing and duration of service usage (calls and/or connections);

- information about amounts of data downloaded and/or uploaded; and

- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

2.3.2 Necessity, proportionality and seriousness

The obtaining of communications data under Part 3 of the Investigatory Powers Act 2016 ("IPA") will be a justifiable interference with an individual's human rights only if the conduct being authorised is necessary for the purposes of a specific investigation or operation, proportionate and in accordance with the law.

Necessity

For a local authority the request to obtain communications data must be necessary for the applicable crime purpose.

Where the communications data sought is wholly or partly events data the purpose must meet the serious crime threshold. A serious crime for the purposed of IPA is:

- an offence for which an adult is capable of being sentenced to one year or more in prison
- any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal
- any offence committed by a body corporate
- any offence which involves, as an integral part of it, the sending of a communication
- any offence which involves, as an integral part of it, a breach of a person's privacy

Where only entity data is sought, the applicable crime purpose is the prevention or detection of crime, or the prevention of disorder.

In order to justify that an application is necessary, the application should as a minimum cover three main points:

(i) the crime under investigation
(ii) the person whose data is sought and how they link to the crime
(iii) the communications data sought and how this data is related to the person and the crime

Proportionality

The following considerations apply:

- whether what is sought to be achieved could reasonably be achieved by other less intrusive means,
- whether the level of protection to be applied in relation to obtaining communications data is higher because of the particular sensitivity of that information, and

- the public interest in the integrity and security of telecommunication systems and postal services.

The degree of collateral intrusion forms part of the proportionality considerations, and becomes increasingly relevant when applying for events data.

Seriousness

In addition to the sentencing threshold, a number of factors should also be considered when applying for communications data:

- the particular circumstances of the case
- the offender
- impact on the victim
- the harm suffered
- the motive for the crime

2.3.3 The Single Point of Contact

The single point of contact (SPoC) is an accredited individual trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority, the Office for Communications Data Authorisations ('OCDA') and telecommunications operators and postal operators. A local authority must use the SPoC at the National Anti-Fraud Network (NAFN).

An applicant within the Council is required to consult a NAFN SPoC throughout the authorisation process.

In addition to being considered by a NAFN SPoC, the applicant must ensure that an officer of at least the rank of the Council's Senior Responsible Officer is aware that the application is being made before it is submitted to an authorising officer in OCDA. The application must be verified by a Council officer of the rank of service manager or above, before it is submitted to an authorising officer in OCDA. The Council's Senior Responsible Officer will inform NAFN of the nominated Council officers who are authorised to verify applications. The authorising officer must be independent from the operation.

NAFN will be responsible for submitting the application to OCDA on behalf of the Council.

The Council can't make an application that requires the processing or disclosure of internet connection records for any purpose.

2.3.4 Applications to obtain communications data

The application to acquire communications data must:

- describe the communications data required, specifying, where relevant, any historic or future dates and, where appropriate time periods;
- specify that the data is required for the applicable crime purpose;
- include a URN;
- include the name and the office, rank or position held by the person making the application;
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect or other person relevant to the investigation or operation;
- include the operation name;
- identify and explain the time scale within which the data is required;
- explain why the acquisition of the data is considered necessary and proportionate;
- present the case in a fair and balanced way;
- consider and, where appropriate, describe any meaningful collateral intrusion;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject of the fact that the application has been made.

2.3.5 Authorisation of applications

An authorising officer in the OCDA will consider an application and record their considerations at the time, in writing or electronically. The authorisation will be granted if the requirements of IPA are met and the acquisition of communications data is necessary and proportionate in the circumstances. If the authorising officer in the OCDA does not consider the criteria for obtaining the data have been met the application will be rejected and/or referred back to the SPoC at NAFN.

Where a request is refused by an authorising officer in OCDA, the Council has three options:

- not proceed with the request;
- resubmit the application with a revised justification and/or a revised course of conduct to acquire communications data;
- resubmit the application with the same justification and same course of conduct seeking a review of the decision by the OCDA. The Council can only resubmit an application on the same grounds where the Senior Responsible Officer has agreed to this course of action.

2.3.6 Duration, renewals and cancellations

The following types of conduct can be authorised - conduct to acquire communications data or the giving of a notice.

An authorisation becomes valid on the date the authorisation is granted. It is then valid for a maximum of one month. This means the conduct authorised should have been commenced which may include the giving of a notice, within that month.

An authorisation may be renewed for a period of up to one month by the grant of a further authorisation.

If an authorisation is no longer necessary or proportionate it must be cancelled. The investigating officer should contact the SPoC at NAFN who will cease the authorised conduct.

2.3.7 Keeping of records

Applications, authorisations, copies of notices, and records of the withdrawal of authorisations and the cancellations of notices must be retained. The council's records are held by NAFN.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely and the requirements of the DPA and the GDPR must be adhered to.

2.3.8 Internal monitoring

The Council's Senior Responsible Officer is [redacted]. The Senior Responsible Officer is responsible for:

- the integrity of the process in place within the Council to acquire communications data;
- compliance with IPA and the code of practice;
- oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner's inspectors when they conduct their inspections; and
- where necessary, oversee the implementation of post-inspection action plans approved by the Commissioner

2.3.9 Oversight

The remit of the Investigatory Powers Commissioner includes comprehensive oversight of the use of powers contained within the IPA. The Investigatory

Powers Commissioner is supported by inspectors in ensuring compliance with the law.

The Investigatory Powers Commissioner must provide an annual report to Parliament on the finding of the inspectors audits, inspections and investigations.

The Investigatory Powers Commissioner will produce guidance for public authorities on how to apply and use investigatory powers.

Further information about the Investigatory Powers Commissioner, their office and their work can be found at: www.ipco.org.uk.

In November 2018 the Home Office published a code of practice – 'Communications Data'. This can be downloaded at

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

Investigation and authorising officers should refer to the code of practice when constructing and considering applications.

Section 3

LONDON BOROUGH OF ISLINGTON

PROCEDURAL NOTE FOR RIPA 2000

APPENDICES

1. Summary checklist of RIPA procedure
2. Checklist for completing authorisation for directed surveillance or a CHIS
3. Court hearing guidance – Briefing sheet

SUMMARY CHECKLIST OF RIPA PROCEDURE

1. An investigation officer identifies the need for directed surveillance or a covert human intelligence source.

2. The investigation officer should complete the relevant authorisation form fully.

3. The authorising officer should satisfy him/herself that the proposed surveillance satisfies the criteria within RIPA and relevant code of practice. The authorising officer should also refer to the council's policy and procedure notes.

4. In the case of a covert human intelligence source, the authorising officer must in addition to the other criteria satisfy him/herself that there is:

   (a) A person who will have day to day responsibility for dealing with the source;
   (b) A person (who can be the authorising officer) who will have the general oversight of the use made of the source.

5. In all cases, the authorising officer, should also be satisfied that there is a person responsible for maintaining and collecting all records to do with the surveillance and authorisation. The authorising officer shall ensure that the officer in the case sends required information regarding the authorisation to Legal Services to be recorded on the central register.

6. The investigation officer(s) are responsible for the storage, maintenance and destruction of the records and authorisations.

7. Upon authorisation, the investigating officer must submit an application for approval to the Magistrates Court.

8. Once the magistrate has approved the authorisation, the investigating officer is entitled to do the activities for the purposes outlined in the authorisation form for the duration of the authorisation.

CHECKLIST FOR COMPLETING AUTHORISATIONS FOR DIRECTED SURVEILLANCE OR COVERT HUMAN INTELLIGENCE SOURCE.

a. Use correct ground(s) for the application
b. Enter sufficient detail of the investigation or operation.
c. Enter sufficient detail regarding the activity proposed.
d. Enter sufficient detail about the criminal offence(s) being investigated, the potential sentence upon conviction and any additional factors which may make the offence more serious. (This only applies in the case of Directed Surveillance)
e. Address the issue of proportionality.
f. Address issue of collateral intrusion and avoid 'rubber stamp' comment.
g. Ensure application signed by the applicant.
h. Authorising Officer should set out clear details of what they are authorising.
i. Authorising Officer should avoid 'rubber stamp' comments.
j. Authorising Officer should record time of when the authorisation was signed.
k. Cancellations should be completed promptly.
l. Ensure review documents are used properly (officers should not use Renewal of Authorisation documents).

Authorisations for directed surveillance should be for 3 months periods. It is possible to state that the authorisation should be reviewed at shorter intervals. If on review, the authorising officer is satisfied that there is no necessity for the authorisation, it should be cancelled.

ISLINGTON

Court Hearing Guidance – Briefing sheet

1. Before the hearing

Read through the authorisation and the application form for Judicial Approval thoroughly.

Ensure you have:

- **The original authorisation plus one copy.**
- **Two copies of the application for Judicial approval**
- **One copy of the Court Order form.**
- **Your personal ID badge**
- **Your delegated authorisation form to appear before the court**

Prepare to explain everything to the Magistrate – remember they may never have seen an application like this before and would not have had time to read the papers. Try and anticipate what questions the Magistrate might ask and have one set of papers ready to hand to the court clerk.

Make sure the Court know you are coming in advance.

2. Arriving at Court

Aim to arrive at court for 9am. Go to the Court Office where the court's legal advisor will check your application and advise you of what court your application will be heard in.

The hearing will be in private - but this is likely to be achieved in the first instance by having a closed court. The judiciary will decide on the day - based on the written application whether further steps should be taken to hold the application in 'chambers'.

3. At the hearing

You should address the Magistrate as 'Sir' or 'Ma'am'. They may be accompanied by a legal adviser who will be a lawyer, often referred to as the Court Clerk.

You should step into the witness box and introduce yourself.

You should be asked to swear an oath (or make an affirmation). This is a matter for the Magistrate's discretion.

The Magistrate may not be familiar with RIPA. Check if the Magistrates would like you to take them through the application. The Magistrate may not find this necessary but they will generally appreciate the offer and say yes

When taking them through the application, or the entire authorisation, explain:

- **The purpose of the application**
- **The covert technique being sought**
- **The criminal offence being investigated**
- **The background to the application**
- **The date and officer who granted the initial authorisation**

In addition to being asked questions by the Magistrates, the Court Clerk may ask you questions.

4. If everything goes well

Ask the Magistrate to sign the order. You need to keep the original authorisation and the original signed order. The Magistrate keeps a copy of everything for the Court records.

5. If the Magistrate is not happy to approve the authorisation

In most cases it is likely that the Magistrate will be happy to approve the authorisation. However, if the Magistrate is not happy to authorise try to get as much information as possible as to why. It might be helpful to ask them if there is any further information which can be provided in support to help persuade them in future.

The Magistrate can:

a) approve the grant or renewal
b) Refuse to approve the grant or renewal, - if the application is refused- the first stage is to check the reasons why and see if it can be easily remedied and then re-apply to the court once the appropriate remedial steps have been taken.
c) Make an order quashing the authorisation - should the Magistrate consider quashing the authorisation, they must give you 2 days' notice to make representations, before they exercise this power.

Whatever the outcome you should take the original authorisation with you when you leave and don't forget to collect your ID badge!