APPENDIX 1

Regulation of Investigatory Powers Act 2000
Use of Covert Surveillance and Covert Human Intelligence Sources

Sovereign Borough Policy

June 2015
Revised May 2016
2nd Revision November 2017
LBHF Version April 2018

1. INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework for police and public authorities to use surveillance and communications data, where necessary and proportionate, for the purpose of preventing or detecting crime. RIPA regulates the use of these powers in a manner that is compatible with the Human Rights Act.

1.2 Officers of the London Borough of Hammersmith & Fulham who want to undertake directed surveillance and or access communications data must do so in accordance with this policy.

1.3 Whilst RIPA itself provides no specific sanction where an activity occurs which should otherwise have been authorised any evidence thereby obtained may be inadmissible in court. The activity may also be unlawful under the Human Rights Act and may result in an investigation by the Ombudsman and/or the Investigatory Powers Tribunal.

1.4 This is a sovereign policy and where the term "the Council" is used it will apply to the London Borough of Hammersmith & Fulham.

1.5 This policy must be read in conjunction with current Home Office guidance issued in December 2014 (see paragraph 14 below).

2. COMMUNICATION DATA

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

2.2 Who or What is a Communications Service Provider?

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

2.3 What is communications data?

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

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

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

2.3.4 Service use data

This includes:

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

2.3.5 Subscriber Information

This includes:

- Name of account holder/ subscriber
- Billing, delivery and installation address(es)
- Contact telephone number(s)
- Bill payment arrangements including bank/credit card details
- Collection/delivery arrangements from a PO box

- Services subscribed to by the customer
- Other customer information such as any account notes, demographic information or sign up data (not passwords)

2.4 Single Points of Contact

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

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

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

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

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

3. DIRECT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

3.1 Part II of Chapter II RIPA deals with Direct Surveillance and Covert Human Intelligence Sources. It covers intrusive surveillance, directed surveillance and use and conduct of Covert Human Intelligence Sources (known as "CHIS") who are more recognisable as agents, informants or undercover officers. The provisions aim to regulate the use of these investigative techniques and to prevent the unnecessary invasion of the privacy of

individuals, essentially to a strike a balance between private and public rights. Please note that neither Council uses CHIS powers (see 3.3 below).

3.2 Surveillance

3.2.1 Surveillance

Surveillance has a broad definition in the Act. It includes:

a) Monitoring, observing or listening to persons, their movements, conversations or other activities or communication. “Persons” includes limited companies, partnerships and cooperatives as well as individuals:

b) Recording anything monitored, observed or listened to in the course of surveillance: and

c) Surveillance by or with the assistance of a surveillance device.

3.2.2 Covert Surveillance

C*overt surveillance* is *surveillance*:

“Carried out in a manner calculated to ensure that persons who are subject to the surveillance are unaware that it is taking place”.

Surveillance which is carried out in the open and is not hidden from the persons being observed does not need to be authorised under RIPA.

3.2.3 Intrusive Surveillance

Local authorities **cannot** carry out or authorise intrusive surveillance in any circumstances. ***Intrusive surveillance*** is surveillance:

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

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

c) Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

Surveillance will not be intrusive if it is carried out by means of a surveillance device designed principally for the purpose of providing information about the location of a vehicle.

3.2.4 Directed Surveillance

RIPA provides that ***directed surveillance*** is surveillance, which is covert and not intrusive and is undertaken:

a) For the purpose of a specific investigation or a specific operation

b) In such a manner likely to result in obtaining ***private information*** about any 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 where it would not be reasonably practical for an authorisation to be sought.

3.2.5 **P*rivate information*** is any information relating to a person's private or family life including his or her relationships with others. The term is broadly interpreted and may include business or professional activities. The fact that covert surveillance is carried out in a public place or on business premises does not mean that it cannot result in obtaining personal information.

3.2.6 When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent "fishing trips". Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been attempted and failed.

3.3 Covert Human Intelligence Sources ('CHIS')

3.3.1 It is council policy of LBHF not to use covert human intelligence sources. It is important that officers understand when the RIPA provisions regarding CHIS come into play so that they can avoid such circumstances.

RIPA defines a person as a CHIS if:

a) S/he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c) below;

b) S/he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) S/he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

3.3.2 A person who reports suspicion of an offence is not a CHIS and they do not become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if they establish or maintain a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

3.3.3 If you believe that using a CHIS is essential for your investigation and you want the Council to depart from the usual policy of not using covert personal relationships you should discuss this with an Authorising Officer

4. AUTHORISATION PROCEDURE

4.1 The Home Office has produced model forms to assist with the requirements of the authorisation process. Copies of the forms, adapted for use by the Councils, are attached at Appendix 3 – 8.

Authorisation must be obtained in relation to each separate investigation. All applications for authorisations, and the authorisations themselves, must be in writing.

4.2 Judicial Approval

4.2.1 The Authorisation does not take effect until the court has made an order approving the grant of the authorisation.

4.2.2 The court has the power to refuse to approve the authorisation and to make an order quashing the authorisation**.**

4.2.3 The Procedure for authorising RIPA applications and seeking Judicial Approval is **at Appendix 1.**

4.3 Authorising Officers/ Designated Person.

4.3.1 RIPA provides that responsibility for authorising directed surveillance, use of a CHIS or acquisition of communication Data lies, within a local authority, with an '**Director, Head of Service, Service Manager or equivalent.**

4.3.4 The following Officers are empowered to act as Authorised persons for applications for surveillance and CHIS, and as Designated Persons for applications for Communication data.

- Tri Borough Head of Fraud
- Bi Borough Head of Environmental Health (Licensing and Trading Standards)
- Head of Community Safety

4.3.5 Authorising Officers should not be responsible for authorising investigations in which they are directly involved.

4.3.6 All Authorising Officers/Designated Persons must have current working knowledge of human rights principles, specifically those of necessity and proportionality,

4.4 Confidential Information

4.4.1 Investigations which may involve "confidential information" must not be conducted without first consulting Legal Services. Confidential information in this context is defined by RIPA and consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

4.4.2 Surveillance involving confidential information cannot be authorised by an Authorising Officer, only the Chief Executive at each Council can authorise surveillance of this nature.

4.5 Necessity and Proportionality

4.5.1 A local authority is required to show that an interference with an individual's right to privacy is justifiable, to the extent that it is both ***necessary and proportionate***.

4.5.2 Directed Surveillance can only be authorised where the Authorising Officer believes, in the circumstances of a particular case, that it is ***necessary*** for the purpose of preventing or detecting crime or of preventing disorder **and** meets the "Crime Threshold" where the criminal offences being investigated meets one of the following conditions:

- The criminal offences, whether on summary conviction or on indictment, are punishable by a *maximum term* of at *least 6 months imprisonment* or an offence under:
- S146 of the Licensing Act 2003 (sale of alcohol to children)
- S147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
- S147A of the Licensing Act 2003 (persistently selling alcohol to children)
- Section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc to persons under 18).

4.5.3 ***Proportionality*** is a key concept of RIPA. The Authorising Officer/Designated Person must also believe that the directed surveillance or use of a CHIS is *proportionate* to what it is sought to achieve. In effect, any intrusion into individual's privacy should be no more than is absolutely necessary.

4.5.4 The authorisation should demonstrate how an Authorising Officer/Designated Person has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut').

.

4.5.5 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 necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented

4.6 Collateral Intrusion

4.6.1 As part of this process an assessment should be made of the risk of what is termed '*collateral intrusion'* - intrusion into the privacy of persons other than those that are the subjects of investigation. Measures should be taken, wherever possible, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation.

4.6.2 If collateral intrusion is inevitable, publication of the material/evidence obtained must be carefully controlled. If the evidence is used in court proceedings, if may be possible to deal with collateral intrusion by editing

5. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATION

5.1 Directed Surveillance

5.1.1 An authorisation for directed surveillance will last **3 months** unless cancelled or renewed and must be cancelled when no longer necessary or proportionate.

5.1.2 Regular reviews of all authorisations must be undertaken to assess the need for the directed surveillance to continue. The results of the review should be recorded on the central register (see below).

5.1.4 Authorisations can be renewed before the date on which they would cease to have effect provided that they continue to meet the relevant criteria. Judicial approval is required for a renewal. The renewal takes effect on the day on which the authorisation would have expired and continues for a **3 or**

12-month period according to the type of activity. Details in relation to any renewal should also be included in the central register.

5.1.5 An Authorising Officer must cancel an authorisation if he or she is satisfied that the activity no longer meets the criteria on which it was based. As before, details of this should be recorded in the central register.

5.2 Communication data

5.2.1 Authorisations and notices for Communication Data will be valid for a maximum of one month from the date of Judicial approval. This means that the conduct authorised should have been commenced or the notice served within that month. All authorisations and notices must relate to the acquisition or disclosure of information for a specific date or period.

5.2.2 Applications can be renewed before the date on which they would cease to have effect provided that they continue to meet the relevant criteria. Judicial approval is required for all renewals. The renewal takes effect on the day on which the authorisation would have expired and continues for a 1 month period.

5.2.3 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application on which the authorisation or notice being renewed was granted or given.

6. CENTRAL RECORD OF AUTHORISATIONS

6.1 The Council must hold a centrally retrievable record of all applications that must be retained for a period of at least 3 years from the ending of an authorisation. This should include the unique reference number ('URN') of the investigation and details of the authorisation, review, cancellation and any renewal. The date of the court order approving the application will also be recorded in the central register.

6.2 The central record is maintained by Chris Reynolds, Community Safety Manager Copies of all relevant documentation relating to applications should therefore be emailed to chris.reynolds@lbhf.gov.uk.

7. SENIOR RESPONSIBLE OFFICER (SRO)

7.1 The Act also requires the Council to have a SRO who is responsible for ensuring compliance with the Act and Code of Guidance and the integrity of the process in place within the authority to acquire communications data. The Chief Officer, Safer Neighbourhoods & Regulatory Services, Environment Department acts as the SRO for the Council.

8. REPORTING

8.1 The Chief Officer, Safer Neighbourhoods & Regulatory Services, Environment Department will report on the use of RIPA annually to the London Borough of Hammersmith & Fulham Transport, Environment and Leisure Select Committee.

8.2 The SRO may, after consultation with the Authorising Officers/Designated Persons, make changes to the list of Authorising Officers/Designated Persons as they consider appropriate in accordance with the requirements of RIPA.

9. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS

9.1 The Authorising Officer/Designated Person should retain RIPA related documents for a period of 3 years. However, where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

10. CCTV

10.1 The general usage of the Council's CCTV system is not affected by this policy. However, if Council officers want to use the Council's CCTV cameras for covert surveillance covered by RIPA then they must have a RIPA authorisation. The Police and Transport for London (TfL) are the only other organisation permitted to use the Council CCTV for RIPA purposes.

10.2 Where the Metropolitan Police wish to use the Council's CCTV system for their own purposes, they shall seek their own authorisation in accordance with Sections 28 or 29 of the Act. In such circumstances authorisation shall usually be obtained from the Superintendent pursuant to the Regulation of Investigatory Powers (Prescription of Officers, Ranks and Positions) Order 2000.

11. POLICY FOR THE CONDUCT OF SURVEILLANCE NOT AUTHORISED BY RIPA

11.1 Following the introduction of the "serious crime threshold" the legal protection offered by RIPA is no longer available in cases where the criminal offence under investigation is not punishable by at *least* 6 months imprisonment. However, this does not mean that it will not be possible to investigate lesser offences or other non-criminal matters with a view to protecting the victim or stopping the offending behaviour or that surveillance cannot be used in such investigations. The statutory RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

11.2 It is recognised that in order to protect residents from serious instances of ASB it may be necessary exceptionally for Council Officers to conduct covert surveillance that does not satisfy the serious crime threshold and cannot be authorised by RIPA. On rare occasions it may also be necessary for Council Officers to conduct covert surveillance when carrying out a disciplinary investigation of an employee. The Office of Surveillance Commissioners guidance, for example, points out in relation to the Police use of intrusive surveillance for the protection of repeat burglary victims and vulnerable pensioners that "the fact that particular conduct [by the authority] may not be authorised under RIPA...does not necessarily mean that the actions proposed cannot lawfully be undertaken, even though without the protection that an authorisation under the Acts would afford". The Investigatory Powers Tribunal has provided clear advice in its judgement in *Addison, Addison & Taylor v Cleveland Police* that where no authorisation is capable of being granted in such circumstances, "it will behove a police force to follow a course similar to that adopted here; i.e. a procedure as close as possible to that which would be adopted if an authorisation could be obtained from a "relevant Authorising Officer". For this reason the Councils have adopted the procedure in Appendix 2 for "non-RIPA" covert surveillance.

11.3 All "non-RIPA" surveillance must be carried out in accordance with the Council Policy for the Conduct of Surveillance Not Authorised by RIPA at **Appendix 2.**

12. SOCIAL MEDIA

12.1 Officers checking Facebook, Instagram, Flickr and other forms of social media as part of an investigation, need to be aware that such activity maybe subject to RIPA either as directed surveillance or deploying a CHIS (see paragraph 3.3.1 above for the definition of a CHIS) and the Councils do not authorise the use of CHIS. Browsing public open web pages where access is not restricted to "friends", followers or subscribers is not covert activity provided the investigator is not taking steps to hide her/his activity from the suspect. The fact that the suspect is or may be unaware of the surveillance does not make it covert. However, any surveillance activity carried out in a manner which is calculated to ensure that a person subject to surveillance is unaware that surveillance against them is taking place is activity which is covert and you will need to consider obtaining a RIPA or NON-RIPA authorisation.

12.2 Officers must not covertly access information on social media which is not open to the public, for example by becoming a "friend' of a person on Facebook, or communicating via social media with the suspect as this type of activity conducted in a covert manner would engage the CHIS provisions which the Councils do not authorise. An example of non-permitted covert surveillance is the creation of a fake profile.

12.3 The gathering and use of online personal information by the Council will engage Human Rights particularly the right to privacy under Article 8 of the European Convention on Human Rights. To ensure such rights are respected the data protection principles in the Data Protection Act 1998 must also be complied with.

12.4 Where online surveillance involves employees then the Information Commissioner's Office's (ICO) Employment Practices Code (part 3) will apply. This requires an impact assessment to be done before the surveillance is undertaken to consider, amongst other things, necessity, proportionality and collateral intrusion. Whilst the code is not law, it will be taken into account by the ICO and the courts when deciding whether the DPA has been complied with.

12.5 This is a constantly evolving subject and officers should discuss any potential use of social media as part of an investigation with Legal Services and Information Management.

13. TRAINING

13.1 Officers conducting surveillance operations, using a CHIS or acquiring communications data must have an appropriate accreditation or be otherwise suitably qualified or trained. Authorising Officers will have received training that has been approved by the Director of Law. All training will take place at reasonable intervals to be determined by the Director of Law but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months

14. THE INSPECTION PROCESS AND OVERSIGHT

14.1 On the 1st September 2017, The Office of Surveillance Commissioners, The Intelligence Services Commissioner's Office and The Interception of Communications Commissioner's Office were abolished by the Investigatory Powers Act 2016. The Investigatory Powers Commissioner's Office (IPCO) is now responsible for the judicial oversight of the use of covert surveillance by public authorities throughout the United Kingdom.

15. FURTHER GUIDANCE

15.1 This policy must be read in conjunction with current Home Office guidance.

Full Codes of Practice can be found on the Home Office website

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers

Further information is also available on The Office of Surveillance Commissioner's website.

http://www.surveillancecommissioners.gov.uk/index.html

Legal advice can be obtained from Legal Services, contacts:
Chief Solicitor(Litigation and Social Care) 0208 753 2744

Appendix 1

PROCEDURE FOR AUTHORISING RIPA APPLICATIONS AND SEEKING JUDICIAL APPROVAL

1 DIRECTED SURVEILLANCE: CRIME THRESHOLD

We can only authorise the use of **directed surveillance** for the following purposes:

- **To prevent or detect criminal offences:**
  - **that are punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months imprisonment** (See page 5 for examples)

  OR
  - **that relate to underage sale of alcohol and tobacco under the following legislation:**
    - **S146 of the Licensing Act 2003 (sale of alcohol to children**
    - **S147 of the Licensing Act 2003 (allowing the sale of alcohol to children)**
    - **S147A of the Licensing Act 2003 (persistently selling alcohol to children)**
    - **Section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc to persons under 18)**

We cannot authorise the use of directed surveillance for the purpose of preventing **disorder** unless this involves a criminal office, whether on summary conviction or on indictment, punishable by a maximum term of at least 6 months imprisonment. (e.g. affray).

On the RIPA Application form **you must**:

1 State you are investigating a criminal offence; and

2 Identify the relevant offence and statute which either punishable with 6 months imprisonment or is related to underage sales of alcohol or tobacco.

Note: that if it becomes clear during an investigation the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the Crime threshold the authorisation **must** be cancelled.

Lesser Offences

In a case where the surveillance has been authorised to investigate a specific offence which meets the threshold but the evidence obtained is used to substantiate offences which fall below the threshold it will be up to the court to decide whether to admit the evidence obtained in

CHIS/ COMMUNICATION DATA

Conduct or use of a CHIS and obtaining communication data can only be authorised where it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

To obtain legal advice call Legal Services for advice:
Janette Mullins, Senior Solicitor (Housing and Litigation):
020 8753 2744

2 PROCEDURE

1. Obtain URN from the , Community Safety Manager Tele
2. Submit Authorisation form to Authorising Officer/Designated Person
   - – Tri Borough Head of Fraud
   - : Bi Borough Head of Environmental Health (Licensing and Trading Standards)
   - : Head of Community Safety

If approval is granted the form to be signed and dated but the **authorisation will not be activated until judicial approval is obtained.**

3. Complete FORM ANNEX B
   This will contain a brief summary of the circumstances of the case but the RIPA authorisation form **must** contain all the information necessary to make application.

4. Telephone the court: Contact Court bookings Manageron 020 3126 3080 to arrange a date/time to attend. The application will be heard by a district judge in chambers.

   Court details:
   Westminster Magistrates court 181 Marylebone Road
   London , NW1 5BR

Email: westminster.mc@hmcts.gsi.gov.uk

Applications will usually be heard at Westminster Magistrates at 10:00am and you must be at court by 9:30am to allow the Legal Adviser to check the application before it goes to court. Go to Court Office on ground floor and explain you have a RIPA Judicial Approval Application.

5. Take with you:
   1 Original and copy of RIPA Authorisation form
   2 Copy of authority to make application.
   3 2 copies of partly completed Form Annex B

6. Hearing
   Sign in with Usher; give him/her the above documents; explain a RIPA Judicial approval application and if you wish to swear on oath or Affirm. Stand in witness box

   - Take, oath or Affirm; identify yourself, name, post, employer
   - Explain you are the investigating officer who has made the application to AO
   - Identify, the AO, Name and post and give date of authorisation.
   - State that you wish to obtain Judicial Approval for Directed Surveillance under S38 Protection of Freedoms Act 2012 and that you have partly completed Form Annex B.
- The Magistrate will consider the following matters:

(a) that the person who granted the authorisation was entitled to do so;
(b) for directed surveillance that the application meets the crime threshold test.
(c) that at the time the authorisation was granted there were reasonable grounds for believing that the surveillance described in the authorisation was—
   (i) **Necessary,** for the purpose of preventing or detecting crime or of preventing disorder
   (ii) **Proportionate** to what was sought to be achieved by it; and
(d) that there remain reasonable grounds for believing those things, at the time the court considers the application.

Necessity and Proportionality

It is still the case that the Authorising Officer must be satisfied that the surveillance is **necessary** for the purpose of "the prevention or detection of crime or the prevention of disorder". This goes beyond the prosecution of offences and includes actions taken to prevent, end or disrupt the commission of criminal offences. But before authorising surveillance the Authorising Officer must be satisfied that officers are investigating an identifiable criminal offence.

The guidance for Magistrates states authorisation will not be **proportionate** if it is excessive in the overall circumstances of the cases. The fact that a suspected offence may be serious will not alone justify surveillance.

No activity should be considered **proportionate** if the information which is sought could be reasonably obtained from other less intrusive means. The risk and proportionality of interfering with the privacy of people not connected with the investigation must also be weighed and, where possible, steps taken to mitigate it.

The Magistrates' guidance suggests that following element of proportionality should be considered:

- Balancing the size and scope of the proposed activity against the gravity or extent of the perceived crime or offence:
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Recording, as far as reasonably practicable, what other methods have been considered and why they were not implemented.

7. **Outcome**

- Application granted and will be effective from date of order.
- Application refused
- Application refused AND quash authorisation – but must give the Council at least 2 days notice from date of refusal to allow us to make representations.

Court will keep 1 copy of Annex form B and 1 copy of Application.

- Provide the , Community Safety Manager Chris Reynolds with a copy of Authorisation form and a copy of Annex B within 5 days of approval.

- Note review date and provide copy of review/and or cancellation to the Community Safety Manager

ANNEX B - RIPA ACCEPTANCE FORM

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority: .....

Local authority department:.....

Offence under investigation: …… .....

Address of premises or identity of subject: .....

.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating
Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP;

.....

Address of applicant department:

.....

.....

Contact telephone number:

.....

Contact email address (optional):

.....

Local authority reference: …….....

Number of pages: .....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' Court ……..

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or

☐ renewal of the authorisation/notice.

refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....
.....
.....
.....
.....
.....
.....
.....

Reasons

.....
.....
.....
.....
.....
.....
.....
.....
.....

Signed:

Date:

Time:

Full name:

Address of Magistrates' Court:

Appendix 2

POLICY FOR THE CONDUCT OF SURVEILLANCE NOT AUTHORISED BY THE REGULATION OF INVESTIGATORY POWERS ACT 2000

London Borough of Hammersmith and Fulham

POLICY FOR THE CONDUCT OF SURVEILLANCE NOT AUTHORISED BY THE REGULATION OF INVESTIGATORY POWERS ACT 2000

The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory framework for the conduct of directed surveillance. It is applicable to local authorities in respect of some of the activities in which they may engage and sets out formal authorisation procedures and codes of practices, with which local authorities should comply.

The Act must be considered in tandem with associated legislation including the Human Rights Act (HRA), and the Data Protection Act (DPA)

The Council has a RIPA policy which is periodically reviewed by Members and the Director of Law.

The purpose of RIPA is to protect the privacy rights of local residents but only to the extent that those rights are protected by the HRA. However, the Council may only engage the Act when performing its 'core functions'. For example, a Local Authority conducting a criminal investigation would be considered to be performing a 'core function', whereas the disciplining of an employee would be considered to be a 'non-core' or 'ordinary' function.

In addition surveillance may only be authorised under RIPA when investigating criminal offences which are punishable by a *maximum term* of at *least 6 months imprisonment* ("the serious crime threshold"). This test was introduced by the Government following concerns that local authorities had been using directed surveillance techniques in less serious investigations, for example, to tackle dog fouling or checking an individual resides in a school catchment area.

Local Authorities have an obligation to deal with Anti-social behaviour (ASB) which involves the day-to-day incidents of crime, nuisance and disorder that make many people's lives a misery. This varies from vandalism, to public drunkenness or aggressive dogs, to noisy or abusive neighbours.

The victims of ASB can feel helpless and in many cases, the behaviour is targeted against the most vulnerable in our society. Even what is perceived as 'low level' anti-social behaviour, when targeted and persistent, can have devastating effects on a victim's life.

To protect residents from ASB it may be necessary for Council Officers to conduct covert surveillance that does not satisfy the serious crime threshold and cannot be authorised by RIPA. For example, graffiti, criminal damage and urinating in public areas can have a real impact on the residents.

To enable the Councils to support victims it is recognised that it may be necessary for the Councils to conduct covert surveillance that does not satisfy the serious crime threshold and cannot be authorised by RIPA.

In addition the Council as Licensing Authority' may need to carry out surveillance of licensed premises in order to promote the four licensing objectives.

On rare occasions it may also be necessary for Council Officers to conduct covert surveillance when carrying out a Disciplinary Investigation of an employee.

When considering covert surveillance which is outside of RIPA Council Officers will, nonetheless, have regard to the Council's RIPA policy, the Directed Surveillance Code of Practice and the OSC Procedures and guidance.

In addition Officers will have regard to the fact that covert surveillance undertaken without RIPA approval, comes with risks e.g.

- evidence unlawfully obtained may be ruled inadmissible and could result in the case collapsing
- a complaint to the RIPA Tribunal
- a complaint to the Local Government Ombudsman
- a claim for damages
- adverse publicity

Investigating Authorising Officers **must** take account of these risks when considering non RIPA surveillance.

Surveillance must not be authorised under this policy if there is any likelihood of acquiring confidential information.

PROCEDURE

- A Council Officer seeking to carry out surveillance outside of RIPA will complete the form attached to this policy

- In completing the form the officer will have regard to the Council's RIPA policy and address the issues of Necessity and Proportionality and "collateral intrusion".

- The form must be passed to one of the Authorising Officers who is empowered to authorise applications made by staff of both Councils.

- The Authorising Officer will consider the application and will decide whether or not to authorise the surveillance applying the principles set out in the RIPA Policy.

- The Non RIPA surveillance must not begin before the date the application is signed by the Authorising Officer.

- The authorised application form must be forwarded to the RIPA co-ordinator Chris Reynolds who will keep a central record of all non RIPA surveillance.

- A monthly review of the authorisation will be conducted to assess the need for the surveillance to continue. The Officer with conduct of the surveillance will submit a review form to the Authorising Officer. The results of the review should be recorded on the central register

- Authorisation for non RIPA surveillance will last **3 months** unless cancelled or renewed and must be cancelled when no longer necessary or proportionate.

- An Authorising Officer must cancel an authorisation if he or she is satisfied that the activity no longer meets the criteria on which it was based.

- The Director of Law in conjunction with the RIPA Coordinator is responsible for ensuring compliance with this procedure and will report on the use of Non RIPA surveillance annually to Members.