London Borough of Hammersmith & Fulham

Regulation of Investigatory Powers Act 2000

Policy for Use of Direct Surveillance and Covert Human Intelligence Sources

June 2015
Revised May 2016
2nd Revision November 2017
3rd Revision November 2019
4th Revision June 2020

CONTENTS

1. INTRODUCTION

1.1. The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory framework for police and public authorities to use surveillance 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 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 2018.

2. DIRECT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

2.1. 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 the Council does not use CHIS powers (see 2.3 below).

2.2. Surveillance

2.2.1. 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.

2.2.2. Covert Surveillance

Covert 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”.

Note: 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.

2.2.3. 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.

2.2.4. 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.

2.2.5. **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. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

2.2.6. 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.

2.3. **Covert Human Intelligence Sources ('CHIS')**

2.3.1. It is Council policy of H&F 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) 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) below;

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.

2.3.2. 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 the person reporting suspicion establishes or maintains a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

2.3.3. 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.

2.3.4. Officers are advised to consult paragraphs 2.17 to 2.26 of the Covert Human Intelligence Sources Revised Code of Practice 2018 which provides further information on when human source activity will meet the definition of a CHIS.

3. AUTHORISATION PROCEDURE

3.1. 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 Council, are attached at Appendices 3 – 6.

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

3.3. **Judicial Approval**

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

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

3.3.3. The Procedure for authorising RIPA applications and seeking Judicial Approval is attached as Appendix 1.

3.4. **Authorising Officers**

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

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

3.4.3. The following Officers are empowered to act as Authorised Persons for applications for surveillance and CHIS:

- Andy Hyatt: Tri Borough Head of Fraud
- Valerie Simpson: Strategic Lead for Environmental Health and Regulatory Services
- Matthew Hooper: Chief Officer for Safer Neighbourhoods & Regulatory Services

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

3.4.5. All Authorising Officers must have current working knowledge of human rights principles, specifically those of necessity and proportionality.

3.4.6. All Authorising Officers are required to attend the necessary training in accordance with section 12 of this policy.

3.5. Confidential Information

3.5.1. 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.

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

3.6. Necessity and Proportionality

3.6.1. 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***.

3.6.2. 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).

3.6.3. ***Proportionality*** is a key concept of RIPA. The Authorising Officer 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.

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

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

3.7. Collateral Intrusion

3.7.1. 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.

3.7.2. 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 appropriate submission.

4. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATION

4.1. Directed Surveillance

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

4.1.2. 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).

4.1.3. 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.

4.1.4. 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. CENTRAL RECORD OF AUTHORISATIONS

5.1. 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.

5.2. The central record is maintained by Stephen Gibbs, RIPA Coordinator. Copies of all relevant documentation relating to applications should therefore be emailed to Stephen.Gibbs@lbhf.gov.uk.

6. SENIOR RESPONSIBLE OFFICER (SRO)

6.1. The Act also requires the Council to have an 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. Sharon Lea, Strategic Director of Environment, acts as the SRO for the Council.

7. REPORTING

7.1. The Head of Community Safety will report on the use of RIPA to the Hammersmith & Fulham Council Community Safety and Environment Policy and Accountability Committee annually.

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

8. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS

8.1. The Authorising Officer 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.

8.2. A copy of all completed RIPA forms, including applications (whether granted or refused), authorisations, reviews, renewals and cancellations, must be forwarded by the Authorising Officer to the RIPA Coordinator.

8.3. Material obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the Council's policies and procedures currently in force relating to document retention.

8.4. All RIPA records, whether in original form or copies must be kept in secure locked storage when not in use.

8.5. All electronic copies of RIPA records, as well as the Central RIPA register, must be stored and shared in accordance with point 8.3. and password protected.

8.6. If there is any doubt regarding information handling and confidentiality, advice should be sought from the RIPA Coordinator or the SRO.

9. CCTV

9.1. 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.

9.2. 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.

10. SOCIAL MEDIA

10.1. Officers conducting online investigations should consult Note 289 on 'Covert Surveillance of Social Network Sites' of the OSC Procedures and Guidance.

10.2. Officers conducting online investigations should also consult paragraphs 3.10 - 3.17 of the Home Office Covert Surveillance and Property Interference Code of Practice 2018.

10.3. Officers checking Facebook, Instagram, Flickr and other forms of social media as part of an investigation, need to be aware that such activity may be 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 Council 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 officers will need to consider obtaining a RIPA or NON-RIPA authorisation. Similarly, repeat viewing of "open source" social media sites may constitute directed surveillance. This should be considered on a case by case basis and officers will need to consider obtaining a RIPA or NON-RIPA authorisation.

10.4. 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. However, this may not apply if the only interaction avoids establishing a relationship by only doing the minimum required to make a test purchase (as per paragraph 10.7 below).

10.5. 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 2018 must also be complied with.

10.6. 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 Data Protection Act (2018) has been complied with.

10.7. Where social media or internet sites are used to investigate the sale of counterfeit goods officers should consider Note 239 on 'Covert Internet Investigations, e-Trading' of the OSC Procedures and Guidance which states: 'CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage'.

11. TRAINING

11.1. Officers conducting surveillance operations or using a CHIS must have an appropriate accreditation or be otherwise suitably qualified or trained. Authorising Officers will have received training that has been approved by the SRO.

11.2. All training will take place at reasonable intervals to be determined by the SRO but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months.

11.3. A log will be kept recording all training received by Authorising Officers and other officers involved in RIPA. This training log will be stored alongside the Central RIPA Register.

12. THE INSPECTION PROCESS AND OVERSIGHT

12.1. 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.

13. FURTHER GUIDANCE

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

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

https://www.gov.uk/government/collections/ripa-codes

Further information is also available on Investigatory Powers Commissioner's Office website

https://www.ipco.org.uk/

Legal advice can be obtained from Legal Services, contacts:

Janette Mullins, Acting 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**

  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 offence, 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 is 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.

CHIS

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

The Authorisation does not take effect until the court has made an order approving the grant of the authorisation. The court has the power to refuse to approve the authorisation and to make an order quashing the authorisation**.**

To obtain legal advice call Legal Services for advice:
Janette Mullins, Acting Chief Solicitor (Litigation and Social Care):
020 8753 2744

2 PROCEDURE

1. Obtain URN from Stephen Gibbs, RIPA Coordinator.
2. Submit Application Form (Appendix 3) to Authorising Officer:
    a. Andy Hyatt: Tri Borough Head of Fraud
    b. Valerie Simpson: Strategic Lead for Environmental Health and Regulatory Services
    c. Matthew Hooper: Chief Officer for Safer Neighbourhoods & Regulatory Services

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 A
   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 Maureen Robertson (Court bookings Manager) on 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 first floor and explain you have a RIPA Judicial Approval Application.

5. Take with you:
   1 Both the original and a copy of RIPA Authorisation form
   2 Copy of authority to make application
   3 Two copies of partly completed Form Annex A

6. Hearing
   Sign in with the Court 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 A

- 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 one copy of Annex Form A and one copy of Application.

- Provide Stephen Gibbs with a copy of Application Form and a copy of Form Annex A within five days of approval.
- Note review date and provide copy of review and/or cancellation forms to Stephen Gibbs.

ANNEX A - 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 – ROLES AND RESPONSIBILITIES

Senior Responsible Officer (SRO)

The SRO is responsible for:

- The integrity of the process in place within the Council for the management of CHIS and Directed Surveillance;
- Ensuring compliance with the Acts and Codes of Guidance;
- Ensuring that a sufficient number of Authorising Officers are, after suitable training on RIPA and this Policy, duly authorised to take action under this Policy;
- Oversight of the reporting of errors to the relevant 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 Office (IPCO) inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

Authorising Officer

- The officers named as Authorising Officers in Section 3.4.3 of this Policy shall be the only officers within the Council who can authorise applications under RIPA in accordance with the procedures set out in this Policy.
- Authorising Officers must ensure that staff who report to them follow this Policy and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this Policy.
- Each of the Authorising Officers can authorise applications, for onward consideration by a Magistrate. Each Authorising Officer may authorise renewals and cancellations, and undertake reviews, in relation to any investigation carried out, or proposed to be carried out, by officers.
- Authorising Officers must have current working knowledge of human rights principles, specifically those of necessity and proportionality.
- Authorising Officers must 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.

- The officer who authorises a RIPA application should also carry out the review, renewal and cancellation. If the original Authorising Officer is not available to undertake the review, renewal or cancellation, this can be undertaken by any other Authorising Officer.

- Authorising Officers must attend training as directed by the SRO.

RIPA Coordinator

The RIPA Coordinator is responsible for:

- The overall management and oversight of requests and authorisations under RIPA;

- Retaining a copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the authorising officer and maintaining a central RIPA records file matrix entering the required information as soon as the forms/documents are received in accordance with the relevant Home Office Code of Practice;

- The issuing of a unique reference number to each authorisation requested under RIPA (this must be before the application has been authorised);

- Reviewing and monitoring all forms and documents received to ensure compliance with the relevant law and guidance and this Policy and informing the Authorising Officer of any concerns;

- Chasing failures to submit documents and/or carry out reviews/cancellations;

- Providing an annual report and summary on the use of RIPA to the Head of Community Safety;

- Organising a corporate RIPA training programme; and

- Ensuring corporate awareness of RIPA and its value as a protection to the council is maintained.

Head of Community Safety (HoCS)

- The Head of Community Safety will report on the use of RIPA to the Hammersmith & Fulham Council Community Safety and Environment

Policy and Accountability Committee annually, and to other panels and committees (where appropriate).

Appendix 3 - RIPA APPLICATION FORM

RIPA Applica

Appendix 4 - RIPA REVIEW FORM

RIPA Revie

Appendix 5 - RIPA RENEWAL FORM

RIPA Renev

Appendix 6 - RIPA CANCELLATION FORM

RIPA Cancell

Appendix 7 - COURT AUTHORISATION LETTER

Court Authori