London Borough of Hammersmith & Fulham

Regulation of Investigatory Powers Act 2000
Policy for Use of Direct Surveillance (Without Judicial Approval / "Non-RIPA")

H&F Version November 2019
1st 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. 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 Human Rights Act.

1.3. 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.

1.4. 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.

1.5. 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.

1.6. 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' ASB, when targeted and persistent, can have devastating effects on a victim's life.

1.7. 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.

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

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

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

1.11. Officers of the London Borough of Hammersmith & Fulham who want to undertake directed surveillance which does not meet the "serious crime threshold" must therefore do so in accordance with this policy.

1.12. Nonetheless, when considering covert surveillance which is outside of RIPA, Council Officers should have regard to the Council's RIPA policy, the Directed Surveillance Code of Practice and the OSC Procedures and guidance (see section **15**).

1.13. In addition, Officers should 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; or
- adverse publicity.

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

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. POLICY FOR THE CONDUCT OF SURVEILLANCE NOT AUTHORISED BY RIPA

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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".

3.6. For this reason, the Council have adopted this policy and procedure for "non-RIPA" covert surveillance. All "non-RIPA" surveillance must be carried out in accordance with this policy.

4. AUTHORISING OFFICERS

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

4.2. The following Officers are empowered to act as Authorising Officers for applications for "non-RIPA" surveillance:

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

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

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

4.5. All Authorising Officers are required to attend the necessary training in accordance with section 16 of this policy.

5. NECESSITY AND PROPORTIONALITY

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***.

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.

5.3. ***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.

5.4. 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').

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

6. COLLATERAL INTRUSION

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.

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 appropriate submission.

7. AUTHORISATION PROCEDURE

7.1. 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 2-4.

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

7.3. A Council Officer seeking to carry out surveillance outside of RIPA must complete the Non-RIPA Application Form attached to this policy (Appendix 2).

7.4. In completing the form, the officer must have regard to this policy and address the issues of Necessity and Proportionality and “collateral intrusion”.

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

7.6. The Authorising Officer will consider the application and will decide whether or not to authorise the surveillance applying the principles set out in this policy.

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

7.8. The authorised application form must be forwarded to the RIPA Coordinator, Stephen Gibbs, who will keep a central record of all RIPA and “non-RIPA” surveillance.

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

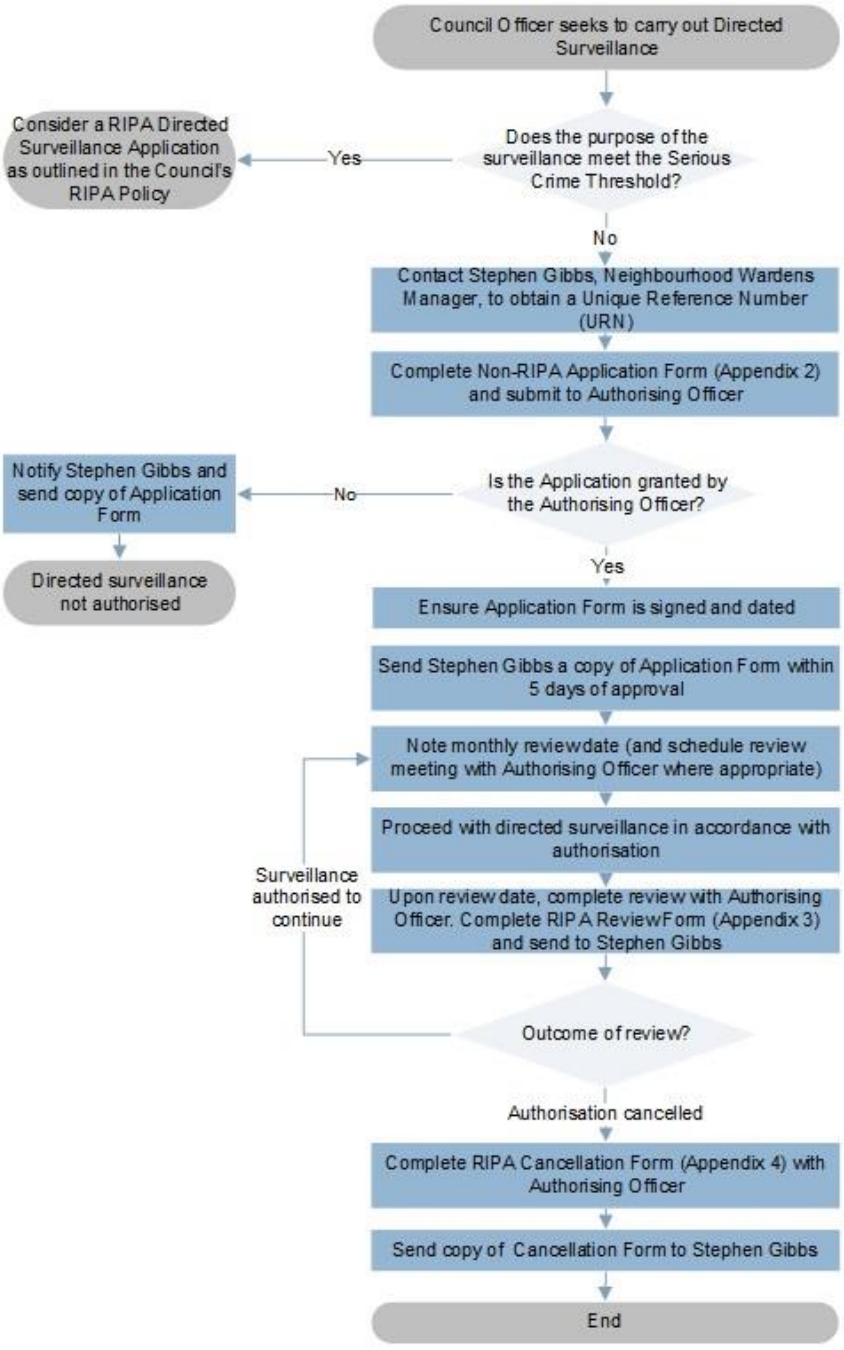
7.10. Authorisation for “non-RIPA” surveillance will last **3 months** unless cancelled or renewed and must be cancelled when no longer necessary or proportionate.

7.11. An Investigating Officer, in liaison with the 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.

7.12. The SRO 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.

8. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATIONS

H&F Non-RIPA Application Process Map



Officer should read RIPA Policy and "non-RIPA" Policy

Note: When considering covert surveillance which is outside of RIPA, Council Officers must have regard to the Council's RIPA Policy, the Directed Surveillance Code of Practice and the OSC Procedures and guidance.

Investigating Authorising Officers must take account of the risks outlined in the "non-RIPA" Policy when considering non-RIPA surveillance.

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

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

Directed Surveillance

8.1. An authorisation for directed surveillance will last **3 months** unless cancelled or renewed (on a month by month basis) and must be cancelled when no longer necessary or proportionate.

8.2. 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.

8.3. Authorisations can be renewed before the date on which they would cease to have effect provided that they continue to meet the relevant criteria. The renewal takes effect on the day on which the authorisation would have expired and continues for **3 months** (or 12 months for CHIS authorisations) according to the type of activity. Details in relation to any renewal should also be included in the central register.

8.4. 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.

9. CENTRAL RECORD OF AUTHORISATIONS

9.1. The Council must hold a centrally retrievable record of all applications for RIPA and "non-RIPA" surveillance 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.

9.2. 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.

10. SENIOR RESPONSIBLE OFFICER (SRO)

10.1. 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.

11. REPORTING

11.1. The Head of Community Safety will report on the use of RIPA (including "non-RIPA" surveillance) annually to the Hammersmith & Fulham Council Community Safety and Environment Policy and Accountability Committee.

11.2. 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.

12. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS

12.1. The Authorising Officer should retain all RIPA (and "non-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.

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

12.3. Material obtained or produced during the course of an investigation 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.

12.4. All RIPA (including "non-RIPA") records, whether in original form or copies must be kept in secure locked storage when not in use.

12.5. All electronic copies of RIPA (including "non-RIPA") records, as well as the Central RIPA register, must be stored and shared in accordance with point 13.3. and password protected.

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

13. CCTV

13.1. 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 or Non RIPA authorisation. The Police and Transport for London (TfL) are the only other organisation permitted to use the Council CCTV for RIPA purposes.

14. SOCIAL MEDIA

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

14.2. 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.

14.3. 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.

14.4. 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).

14.5. 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.

14.6. 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.

14.7. 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'.

15. FURTHER GUIDANCE

15.1. This policy must be read in conjunction with:

- the Council's RIPA policy which gives more detail about directed Surveillance and CHIS
- 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, Chief Solicitor (Litigation and Social Care) 0208 753 2744

Appendix 1 – 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 (including "non-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 (including “non-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 (including “non-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 (including “non-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, including “non-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 (including “non-RIPA”) to the Head of Community Safety;

- Organising a corporate RIPA training programme; and

- Ensuring corporate awareness of RIPA (including “non-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 (and “non-RIPA”) annually to the Hammersmith & Fulham Council Community Safety and Environment Policy and Accountability Committee, and to other panels and committees (where appropriate).

Appendix 2 – NON-RIPA APPLICATION FORM

Non-RIPA appl

Appendix 3 – NON-RIPA REVIEW FORM

Non-RIPA re

Appendix 4 – NON-RIPA RENEWAL FORM

Non-RIPA rei

Appendix 5 – NON-RIPA CANCELLATION FORM

Non-RIP