BARNET
LONDON BOROUGH

Counter Fraud Framework Manual 2014

Regulation of Investigatory Powers (RIPA) Policy Statement and Procedure - Directed Surveillance

Document Control

Document Description	Counter Fraud Framework Manual – RIPA Policy Statement and Procedure	
Project Name	LBB / CAFT / CFF / 2014	
Version	V2	
Date Created	October 2014	
Status	Draft	
Prepared By:	Clair Green –Assurance Assistant Director	October 2014
Approved By:	Strategic Commissioning Board	October 2014
Approved By:	Audit Committee	TBC

Version History

Version number	Date	Author	Reason for New Version
Version 1 2013 Final Issued	May 2013	Clair Green	2013 Update
Version 2 2014	October 2014	Clair Green	Annual Review

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") and regulations made under that Act provide a statutory framework for the use of covert investigation techniques by public authorities.

1.2 The Council is permitted to conduct directed surveillance and use covert human intelligence sources having first complied with the requirements of RIPA. In doing so it will make lawful any conduct authorised and carried out in accordance with the procedural requirements. If RIPA is not followed it does not necessarily make conduct carried out under it unlawful, but it does provide evidence to justify why an individual's rights under Human Rights legislation and case law have been interfered with. Compliance with RIPA may demonstrate that such interference was in accordance with the law, necessary and proportionate in accordance with Article 8(2) of the Human Rights Act. It should also be noted that if correct procedures under RIPA are not followed, the evidence gathered may be judged inadmissible in any subsequent legal proceedings or a complaint of maladministration might be made. It is essential therefore that all officers involved in surveillance of a covert nature should adhere to the Council's policy and procedures.

1.3 Regard must also be had to other provisions as detailed in the council's Information Governance Policies the Data Protection Act 1998 and its Code of Practice, the Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

1.4 If an officer has any doubt whether RIPA applies or about the process to be followed or other related legislative provisions, advice should be sought from the Legal Gatekeeper (see 9.3 below).

1.5 The Council must have regard to the guidance contained within the statutory Codes of Practice published by the Secretary of State. The Codes of Practice provide detailed guidance on the matters addressed in this policy. Example scenarios are provided which demonstrate the practical application of RIPA considerations. The Codes of Practice are available from the Home Office website: http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

2 Surveillance

2.1 Surveillance includes:

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications
- recording anything mentioned above in the course of authorised surveillance
- surveillance, by or with, the assistance of appropriate surveillance device(s).

2.2 RIPA is concerned solely with the regulation of *covert* surveillance. Therefore surveillance which is conducted in an overt manner is not covered. For example, CCTV cameras used in town centres which are clearly signposted and not concealed from public view will not be subjected to RIPA authorisation. However, their use may be covered by RIPA if used for the purpose of a specific operation or investigation. If the Police or other law enforcement agency request use of the Council's CCTV system for their operation, any surveillance undertaken would normally be carried out subject to prior RIPA authorisation having been obtained by that authority.

- **Covert surveillance** is surveillance that is carried out in a manner calculated to ensure that the person(s) subject to the surveillance are unaware that it is or may be taking place. Surveillance can be directed or intrusive.

- **Directed surveillance** is:
  i. covert
  ii. not intrusive (see description below)
  iii. is undertaken for the purposes of a specific investigation
  iv. is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
  v. is not an immediate response to events which would otherwise make seeking an authorisation under the Act unreasonable for example where officers observe criminal activity during the course of their routine duties and conceal themselves to observe what is happening

2.3 The Council **must not** carry out intrusive surveillance. **Intrusive surveillance** is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle; and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

2.4 **Private information** about a person includes any information relating to his private or family life, professional or business relationships, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not automatically mean that it cannot result in the obtaining of private information about a person.

3 Covert Human Intelligent Source

3.1 A **Covert Human Intelligence Source** ("CHIS") is a person who establishes or maintains a personal or other relationship for the covert purpose of using the relationship to obtain information or to provide access to any information about another person or for covertly disclosing information obtained by the use of such relationships.

3.2 The Council can only use a CHIS subject to the procedures detailed in this policy being followed.

3.3 A CHIS will usually include undercover officers and those who carry out test purchases. However, the Code of Practice on CHIS suggests that a young person carrying out a test purchase at a shop is unlikely to be construed as a CHIS based on a single transaction.

3.4 The Council does not usually make use of CHIS. However, officers must bear in mind the possibility of a CHIS arising in circumstances where it was not contemplated. A member of the public volunteering information as part of their normal civic responsibility would not normally considered to be a CHIS. However, if specific instructions are provided to that member of the public a CHIS situation may arise. Advice should be sought from the Gatekeeper (see 9.3 below).

Juvenile/Vulnerable individuals

3.5 Special considerations apply to the use or conduct of juvenile sources (i.e. under 18 years old) or vulnerable individuals. On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Advice should be sought from the Gatekeeper (see 9.3 below) prior to any intended use.

Managing a CHIS

3.6 One person within the relevant service area is, following authorisation, to be tasked with the day to day running of the CHIS, contact with them, giving them tasks and keeping confidential records of what they achieve and a separate person identified to oversee the use made of the CHIS.

3.7 A risk assessment must be carried out in relation to security and welfare of the CHIS. This assessment should take place before any application for authorisation is made, at any renewal, review and cancellation.

4 Partner Organisations and Contractors and Third Parties

4.1 The Council retains overall responsibility for any surveillance activities undertaken by third parties assuming the Council's functions such as Barnet Homes which is an Arms Length Management Organisation ("ALMO") that manages the Council's public sector housing stock.

4.2 Partner organisations, contractors and any other third parties carrying out Council functions must comply with the requirements outlined within this policy.

4.3 Any applications for directed surveillance or use of a CHIS by partner organisations must be approved by an Authorising Officer of the Council in the normal manner.

4.4 Any queries relating to the role and responsibility of such organisations or individuals must be directed to the Gatekeeper.

5. Authorisation

5.1 An authorisation under RIPA ensures that directed surveillance and the use of a CHIS is lawful so long as the conduct is in accordance with such authorisation. The flowcharts at Appendices 1 and 2 provide a guide as to when authorisation is required.

5.2 Authorisation will only be granted if necessary **and** proportionate.

5.3 Consideration of **proportionality** includes determining whether the proposed conduct is proportionate to what it seeks to achieve and whether it is excessive in the overall circumstances of the case. Consideration must be given as to whether the information sought could be obtained by less intrusive means.

5.5 The Council is only permitted to undertake directed surveillance or use a CHIS if it is for the prevention or detection of crime. The investigating officer should therefore identify the suspected criminal offence at the outset of the investigation.

5.6 Authorisation for directed surveillance can only be granted where the Council is investigating particular categories of criminal offences. This is referred to as the **Crime Threshold Test**. These categories are:

- Criminal offences which attract a maximum custodial sentence of six months or more
- Criminal offences relating to the underage sale of alcohol or tobacco contrary to s146, s147 and 147A Licensing Act 2003 and s7 Children and Young Persons Act 1933

5.7 The criminal offence under investigation must be identified by the investigating officer by statute and section in the authorisation form so the Authorising Officer can check that this requirement has been satisfied.

5.8 The Crime Threshold Test does not apply to authorisations for use of a CHIS.

5.9 If during the investigation it becomes clear that the activity being investigated is a less serious offence that does not meet the above threshold, the directed

surveillance should immediately cease. If a directed surveillance authorisation is already in force it should be cancelled.

6. Authorisation Procedure

6.1 The investigating officer must complete the Home Office approved RIPA application form for either directed surveillance or use of a CHIS. Should the officer completing the form require any assistance or have any queries, they should contact the Gatekeeper or Authorising Officer (see 9.3 and 9.5 below).

6.2 The investigating officer should obtain a unique reference number (URN) from an Authorising Officer prior to the authorisation form being sent to that officer.

Authorisation by Authorising Officer

6.3 The completed application form must be sent to an Authorising Officer (see 9.3 below) for approval.

6.4 An Authorising Officer will only approve an authorisation if the conduct in question is necessary and proportionate.

6.5 The Authorising Officer will also consider the likelihood of collateral intrusion i.e. the risk of obtaining private information about persons who are not the intended subject of the surveillance. Measures should be taken to avoid or minimize unnecessary intrusion.

6.6 The Authorising Officer must also consider whether any confidential information is likely to be acquired i.e. information held in confidence relating to the physical, mental health or spiritual counseling of a person (whether living or dead).

6.7 In the highly unlikely event that an authorisation is sought for directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person as a CHIS requires authorisation by the Head of Paid Service i.e. the Chief Executive or Acting Chief Executive.

Judicial Approval

Once the Authorising officer has approved the authorisation, the next stage is to obtain Judicial Approval of the directed surveillance or use of a CHIS in order to activate the authorisation. This requirement was introduced from 1 November 2012 by the Protection of Freedoms Act 2012. Officers must note that any directed surveillance or use of a CHIS **must not** commence until Judicial Approval has been granted, as the authorisation does not take effect until an order approving the grant of the authorisation has been made by a Justice of the Peace i.e. District Judge or lay magistrate.

6.8 Judicial Approval will be by way of an order approving the grant of the authorisation for directed surveillance or use of a CHIS. The Justice of the Peace will only issue an order if satisfied that the statutory tests have been met and that the proposed conduct is both necessary and proportionate.

6.9 The same Judicial Approval process is required for renewal applications.

Procedure for Applying for Judicial Approval

6.10 Following approval from the Authorising Officer the investigating officer must contact Willesden Magistrates Court to arrange a hearing.

6.11 The investigating officer must attend the hearing and provide the Justice of the Peace with the following:

- the original RIPA authorisation approved by the Authorising officer (this must be retained by the officer for the Central Register)
- copy of the RIPA authorisation for retention on the Court file
- supporting documents setting out the case

6.12 Partially completed judicial application/order form as appears at Annex B of the Home Office guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance October 2012 which can be found on the Home Office website

6.13 The investigating officer must be formally designated to appear before the Magistrates.

6.14 The Justice of Peace will consider whether he/she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will then consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation was an appropriate designated person within the Council and that the authorisation was made in accordance with any legal restrictions e.g. the crime threshold for directed surveillance.

6.15 The Justice of the Peace may decide to:

- Approve the grant or renewal of an authorisation – the authorisation will then take effect
- applies restrictions if decides to on application and authorisation
- Refuse to approve the grant or renewal of an authorisation – the authorisation will not take effect and the Council will **not** be permitted to carry out the directed surveillance or use the CHIS
- Refuse to approve the grant or renewal of an authorisation and quash the authorisation – however the Court must not quash the authorisation unless the Council has received at least 2 working days notice from the date of the refusal to make representations

6.16 If an application has been refused for a technical reason, for example, where a document was not available at the hearing, the Council may consider reapplying for Judicial Approval

6.17 The order section of this form will be completed by the Justice of the Peace and will be the official record of the decision. The Council must retain a copy of the signed judicial application/order form.

6.18 Appendix 3 is a flowchart showing the procedure to follow when seeking Judicial Approval.

6.19 Central Register of all original authorisations, renewals, reviews and cancellations is maintained by the Authorising Officer (see 9.3 below). Each Service area must also ensure copies of each these documents is stored within the relevant files. The Central Register will be maintained for at least three years from the ending of each authorisation.

7 Duration of Authorisations, Renewal and Cancellation

7.1 Authorisations for directed surveillance last for three months and authorisations for use of a CHIS for 12 months (1 month if the CHIS is under 18) from the date of Judicial Approval.

7.2 The authorisations do not expire, they must be reviewed and/or cancelled once they are no longer required.

7.3 Any renewal application for the authorisation must be made prior to the expiry of the original authorisation. The tests of necessity and proportionality will be reapplied by the Authorising officer prior to submission to a Justice of Peace for Judicial Approval.

7.4 Renewals may be granted Judicial Approval more than once if still considered necessary and proportionate.

7.5 Authorisations must be cancelled in writing as soon as the authorisation is no longer required.

7.6 Officers must use the Home Office approved RIPA forms for application, renewals and cancellations. These forms can be obtained directly from an Authorising Officer, the legal gatekeeper or via the Home Office website.

8 Designated Officers – Roles and Responsibilities

8.1 Senior Responsible Officer

The Council's Senior Responsible Officer ("SRO") has been designated as the Council's monitoring Officer / Director of Assurance. The SRO's role includes:

8.3.1.1 maintaining an oversight of RIPA procedure and requirements

8.3.1.2 providing quality assurance regarding the use of directed surveillance and CHIS including overseeing the competence of Authorising Officers

8.3.1.3 engaging with the Commissioners and Inspectors of the Office of Surveillance Commissioners when they conduct their inspections

8.3.1.4 where necessary oversee the implementation of any post-inspection action plans

8.2 Authorising Officers

The Council has designated the following officers as having the power to grant authorisations for the carrying out of directed surveillance and the use of a CHIS: the Assurance Assistant Director and the CAFT Counter Fraud Managers.

The Authorising Officers' role includes:

1. applying the statutory tests and granting authorisations for directed surveillance and the use of CHIS if considered appropriate
2. identifying training needs of Council officers
3. responsibility for raising awareness of RIPA throughout the Council
4. maintaining the Central Registers of directed surveillance and CHIS authorisations
5. maintaining an equipment register detailing the issue and receipt of the Council's technical equipment used for surveillance
6. providing training to investigating officers as necessary

8.3 Gatekeeper

The Gatekeeper is a designated legal officer within the councils Shared Legal Service HB Public Law. The Gatekeeper's role includes:

1. providing advice and assistance to both Authorising Officers and Investigating Officers
2. keeping abreast of updates and changes to RIPA, associated legislation, Codes of Practice and any Guidance issued. The Gatekeeper will notify the SRO and Authorising Officers of such changes.

9 Raising a concern

Access to communications data

9.1 RIPA also regulates access to communications data held by telecommunication service operators. The Home Office website has a link to the relevant Code of Practice.

9.2 The Council is permitted to access only subscriber information and service data only where it is required for the purpose of preventing or detecting crime.

9.3 The Council uses NAFN which is an accredited organisation to deal with telecommunication data requests. The use of NAFN ensures that the Council's statutory responsibilities for compliance with RIPA and associated legislation is complied with. NAFN operate a secure online system for processing and assessing communication data requests.

9.4 The requesting officer will initially complete an application form on the NAFN online system using their secure login. NAFN will then carry out statutory checks prior to authorisation being sought from the Authorising Officer. The Council's nominated Authorising Officer is the Assistant Director of Assurance. If authorisation is granted by the Authorising Officer, the requesting officer must then seek Judicial Approval prior to the data being obtained via NAFN.

10 Other relevant Barnet policies

10.1 Counter Fraud Framework Manual and introduction document

- Fraud Policy Statement and Procedure
- Bribery Policy Statement and Procedure
- Whistleblowing Policy Statement and Procedure
- Prosecution and Sanction Policy Statement
- Anti Money Laundering Policy Statement and Procedure

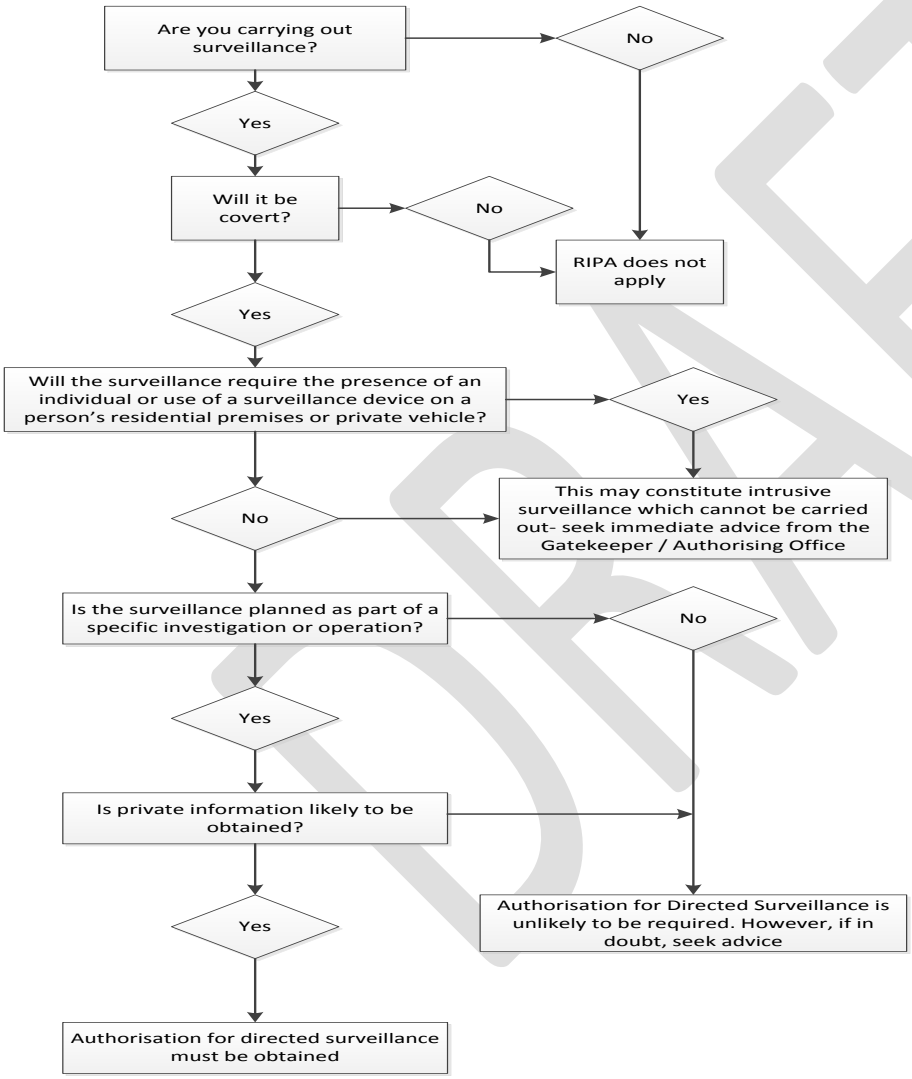
10.2 Information Governance Policies

10.3 Staff Code of Conduct

APPENDIX 1

Determination of Whether Directed Surveillance Authorisation is Required

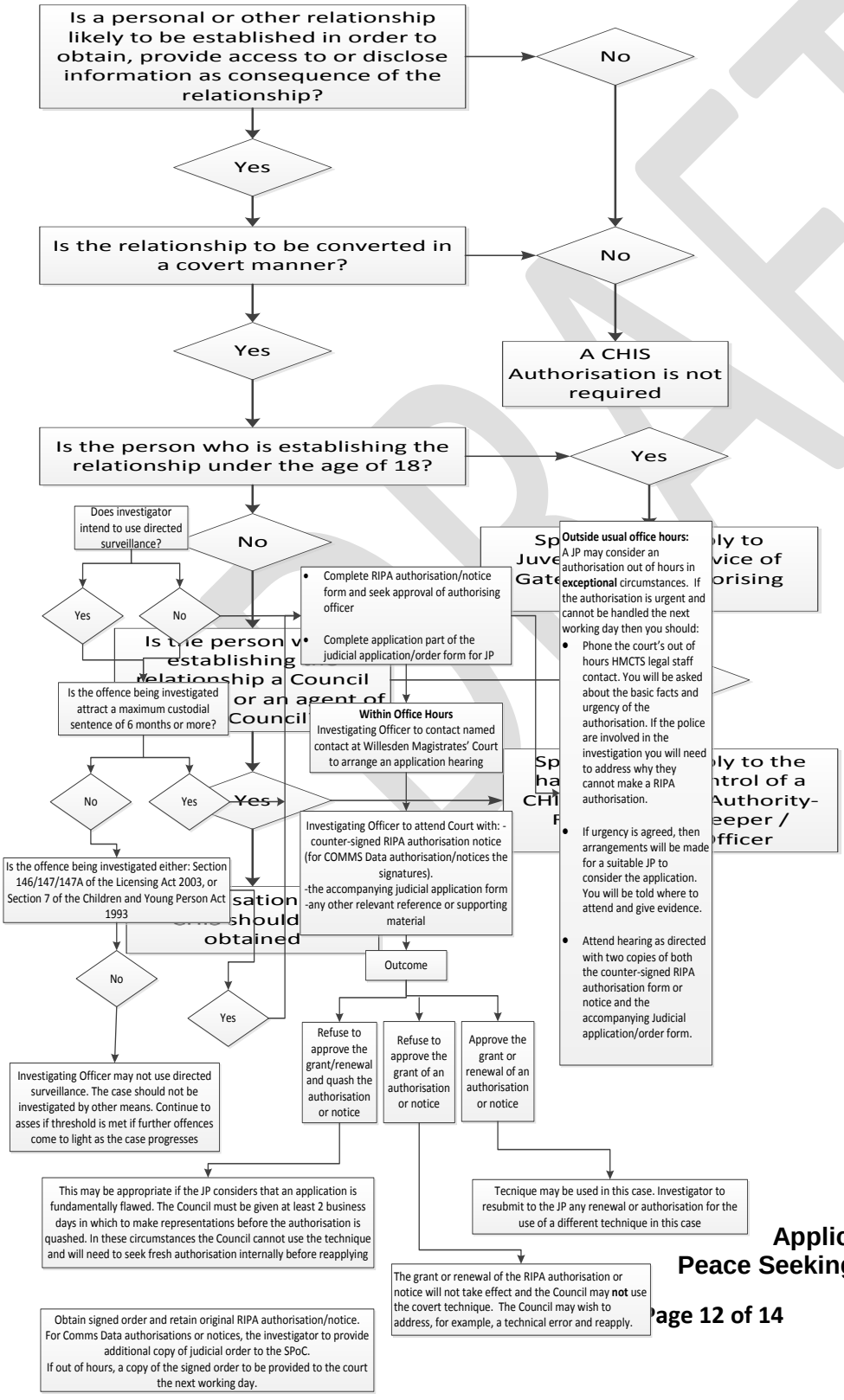
(Please note this is only provided as a brief summary. Any queries should promptly be referred to the Gatekeeper or Authorising Officer)



APPENDIX 2

Determination of Whether CHIS Authorisation is Required

(Please note this is only provided as a brief summary. Any queries should immediately be referred to the Gatekeeper or Authorising Officer)



APPENDIX 3

Application to a Justice of the Peace Seeking an Order to Approve the

Grant of a RIPA Authorisation for Directed Surveillance, CHIS or Communications Data