



Haringey Council

Report for:	Cabinet 10 September 2013	Item number	
Title:	Regulation of Investigatory Powers Act (RIPA) 2000 – use within the Council 2012/13 and amendments to the Council's policy and procedures		
Report authorised by :	Director of Corporate Resources <i>J. Parker 29/8/13</i>		
Lead Officer:	Anne Woods, Head of Audit and Risk Management Tel: 020 8489 5973 Email: anne.woods@haringey.gov.uk		
Ward(s) affected: ALL	Report for: Non-Key Decision		

1. Describe the issue under consideration

1.1 To inform Cabinet about issues relevant to the use of the Regulation of Investigatory Powers Act (RIPA) 2000 during 2012/13 and provide an updated policy for approval.

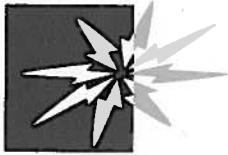
2. Cabinet Member for Finance and Carbon Reduction Introduction

2.1 The Protection of Freedoms Act 2012 introduced the requirement for judicial approval to be obtained prior to directed surveillance being undertaken. The Council uses this facility infrequently, but needs to comply with legislation and report the use of directed surveillance to members on an annual basis. I am satisfied that the Council uses the powers afforded to it under the RIPA legislation appropriately, as signified by the approval of all requested directed surveillance since the new legislation came into effect.

2.2 The changes to the policy incorporate the new legislation requirements and accord with Home Office guidelines and on that basis I recommend that Cabinet approve these.

2. Recommendations

3.1 The Cabinet notes the use of RIPA by the council in 2012/13;



3.2 The Cabinet approves the amended RIPA policy and procedures at Appendix 1 and agrees that the officers listed in the appendix to Appendix 1 be permitted to authorise directed surveillance and the use of covert intelligence under s.28 and S.29 of RIPA 2000 prior to judicial approval; and

3.3 The Cabinet notes that the Director of Corporate Resources is the Senior Responsible Officer for oversight of RIPA in accordance with Home Office guidance.

3. Other options considered

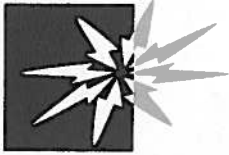
4.1 Not applicable.

4. Background information

5.1 On 25 September 2000 the Regulation of Investigatory Powers Act (RIPA) was brought into effect in England and Wales. The purpose of the Act was to ensure that all public authorities were able to carry out directed (covert) surveillance on a statutory basis without breaching The Human Rights Act 1998, Article 8, the right to privacy. RIPA enables local authorities to carry out certain types of surveillance activity as long as specified procedures are followed. The information obtained as a result of surveillance operations can be relied upon in court proceedings provided RIPA is complied with.

5.2 On 1 May 2012, the Protection of Freedoms Act 2012 received Royal Assent. This legislation requires local authorities to obtain judicial approval before using RIPA. Secondary legislation brought this new requirement into law on 1 November 2012. Since this date, all applications must also be authorised by a Justice of the Peace before they can take effect and the Council has to apply to the Magistrates Court to grant an order approving the authorisation. This requirement applies to all areas of RIPA, including directed surveillance, and communications data.

5.3 In addition, the new legislation limits the use of RIPA to offences that have a custodial sentence of six months or more, with some exceptions relating to the sale of alcohol and tobacco to children. The Council's RIPA policy has been revised to reflect the changes and a copy of the revised policy is attached at Appendix 1.



Haringey Council

5.3 The use and application of RIPA legislation is monitored by two government offices who both report to parliament and the Secretary of State. The Office of the Surveillance Commissioner (OSC) monitors the use of RIPA in relation to directed surveillance. The Interception of Communications Commissioner's Office (IOCCO) is responsible for monitoring the use of RIPA in relation to communications data. Visits are made to local authorities to monitor compliance with RIPA legislation by both the OSC and the IOCCO. Both organisations require annual returns and performance information to be made by the Council.

5.4 The Code of Practice on Covert Intelligence Sources states that elected members should review the authority's use of RIPA at least once a year.

5. Operational Procedures in Haringey

6.1 The Home Office Code of Practice recommends that a member of the organisation's corporate leadership team should be the Senior Responsible Officer for oversight of RIPA. Within Haringey, the Senior Responsible Officer is the Director of Corporate Resources, who has been provided with guidance on the role and responsibilities.

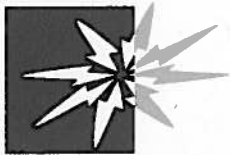
6.2 It is proposed that the officers listed in the appendix to Appendix 1 approve RIPA forms prior to seeking judicial approval. These officers have been trained in the use and application of RIPA. Refresher training is provided on a regular basis to ensure all officers are kept up to date with their roles and responsibilities.

6.3 Haringey has produced its own local guidance notes for RIPA, which are in accordance with the Home Office's requirements; and these are circulated to all officers involved in RIPA when updates to the legislation or standard forms are issued. These guidance notes are also published on the Council's intranet site. Previous OSC inspections have confirmed that Haringey's policy is in line with Home Office guidance.

6.4 Haringey makes limited use of RIPA legislation and the Council has always complied fully with the legislative requirements. A summary of the total number of applications to use RIPA from 2010/11 to 2012/13 is detailed in Table 1 below.

Table 1

Year	2010/11	2011/12	2012/13
Department			
Place & Sustainability	3	1	8
Corporate Resources	0	0	1
Total	3	1	9



Haringey Council

6.5 Table 2 below provides details of the use made of RIPA during 2012/13. All requirements of RIPA have been fulfilled and relevant returns to the OSC and IOCCO have been completed for 2012/13.

Table 2

Department	Use applied for	Application authorised
Place & Sustainability	To investigate serious anti-social behaviour causing injury to residents of a housing scheme	Y
Place & Sustainability	To identify serial arsonist at housing block causing damage to properties and potential risk to tenants	Y
Place & Sustainability	To investigate serious anti-social behaviour causing criminal damage to housing blocks	Y
Place & Sustainability	To investigate serious anti-social behaviour and alleged drug dealing at housing blocks	Y
Place & Sustainability	To identify serial arsonist at housing block causing damage to properties and potential risk to tenants	Y*
Place & Sustainability	To identify serial arsonist at housing block causing damage to properties and potential risk to tenants	Y*
Place & Sustainability	To identify arsonist at housing block causing damage to properties and potential risk to tenants	Y*
Place & Sustainability	To identify arsonist at housing block causing damage to properties and potential risk to tenants	Y*
Corporate Resources	To investigate allegations of serious Housing Benefit and housing tenancy fraud	Y
Total		9

*application made after 1/11/12 and subject to judicial approval

7. Comments of the Chief Financial Officer and Financial Implications

7.1 There are no direct financial implications arising from this report. The work within internal audit and other departments to undertake and manage RIPA in accordance with statutory requirements is contained and managed within the relevant revenue budgets.

8. Legal Implications

8.1 The Head of Legal Services has been consulted in the preparation of this report. The legal issues arising have been covered in the body of this report.

9. Equalities and Community Cohesion Comments

9.1 There are no direct equality implications arising out of this report. The revisions outlined in the Protection of Freedoms Act 2012 strengthen existing Human Rights legislation, protecting individuals from inappropriate levels of covert surveillance.

10. Head of Procurement Comments

10.1 Not applicable.



Haringey Council

11. Policy Implications

11.1 There are no direct implications for the Council's existing policies, priorities and strategies.

12. Use of Appendices

12.1 Appendix 1 – RIPA Policy and Procedures 2013.

**REGULATION OF
INVESTIGATORY
POWERS ACT 2000
HARINGEY COUNCIL
PROCEDURE AND
GUIDANCE NOTES
April 2013**

Author:	Anne Woods
Owner:	Anne Woods
Version:	9.2
Classification:	UNCLASSIFIED
Issue Status:	FINAL
Date of First Issue:	2004
Date of Latest Re-issue	22/04/2013

Contents

Section	Title	Page
	Glossary of terms	3
	- 1 Introduction	6
Section A	General procedures <ul style="list-style-type: none"> - 2 Undertaking Covert Surveillance - 3 Senior Responsible Officer (SRO) - 4 Authorisation Office (AO) - 5 Collateral Intrusion - 6 Risk Assessment - 7 Health & Safety - 8 Procedure on Directed Surveillance - 9 Procedure for the use of surveillance equipment - 10 Intrusive Surveillance - 11 Procedure for Monitoring and reviewing RIPA - 12 Procedure for data retention - 13 Central Record of Authorisations - 14 Complaints Handling - 15 Training - 16 Data Protection 	8 9 9 9 10 10 10 13 16 16 16 17 17 18 18
Section B	Communications Data procedures <ul style="list-style-type: none"> - 1 Communications Data Section B Tables <ul style="list-style-type: none"> - NAFN Example web application form 	19 22
Section C	CHIS procedures <ul style="list-style-type: none"> - 1 Procedure for Covert Human Intelligence Source(CHIS) 	24
	Appendix 1 – Authorisation Officers for Haringey Council	28

Glossary of Terms

RIPA 2000. Regulation of Investigatory Powers Act 2000.

Protection of Freedoms Act 2012. Sections 37 and 38 of the Act apply, from 1 November 2012, to local authorities who wish to use directed surveillance, acquire communications data or use a covert human intelligence source (CHIS).

Senior Responsible Officer (SRO). An SRO is an officer within the Council who is a member of the Corporate Board and is responsible for the integrity of the processes in place within the Council for the management of RIPA.

Authorisation Officer (AO). There are specific statutory requirements regarding the authorisation of specific activities under the RIPA legislation. A list of relevant AO's for the Council is shown at Appendix 1. The AO's can authorise applications for both directed surveillance and communications data prior to submission to a Justice of the Peace for final approval.

Investigating Officer (IO). An IO is an Officer within the Council who is involved in undertaking a specific investigation or operation.

Designated Person (DP). The Designated Person considers the Communications Data applications and records their considerations. The DP is the equivalent of the AO for directed surveillance.

Communications Service Provider (CSP). A CSP is an operator who provides a postal or telecommunications service as defined in RIPA 2000.

Covert Surveillance. Covert Surveillance is either Directed Surveillance or conducting surveillance with the use of a Covert Human Intelligence Source. Covert Surveillance is not intrusive, but it is likely to obtain private information about a person.

Directed Surveillance. Directed Surveillance is defined under section 26(2) of RIPA. Surveillance is directed if it is covert but not intrusive and is undertaken for the purpose of a specific investigation or a specific operation and is likely to involve the obtaining of private information about a person. This could include the use of an overt CCTV system for a directed and specific covert purpose.

CHIS. CHIS is defined as a Covert Human Intelligence Source and is subject to statutory control under section 29 of the RIPA Act 2000. A CHIS is a person who is required to establish or maintain a personal or other relationship with someone to obtain information in order to assist an investigation. Other relationships can include professional, business or working relationship. A CHIS is therefore the person who acts covertly and passes information to the designated handler.

Designated Handler. A designated handler is responsible for directing the day to day activities of the CHIS as well as the security and welfare of the CHIS.

Intrusive Surveillance. (Available only to Police or other law enforcement agencies). Intrusive surveillance is surveillance undertaken covertly which is carried out in relation to anything taking place on residential premises without the persons consent; or in any private vehicle and must involve the presence of an individual on the premises or in the vehicle, and may be carried out by the means of a surveillance device.

Private Information. Includes any information relating to a person's private or family life. This includes the right to establish and develop relationships with other human beings and activities that are of a business or professional nature.

Private Vehicles. Private Vehicles are subject to RIPA where any vehicle is used primarily for the private purposes of the person who owns it or for a person otherwise having the right to use it.

Residential Premises. Residential Premises are subject to RIPA, where premises are being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used).

Necessity. Necessity requires that covert surveillance take place when there are no reasonable and effective alternative (overt) means of achieving the desired objective.

Proportionality. If the activities are necessary then the AO must believe that the activity is proportionate to the likely outcome. The AO must balance the intrusiveness of the activity on the target and others who might be affected by it, against the need for the activity in operational terms. The activity will not be proportionate if it is considered excessive in the circumstances of the case, or if the information could have reasonably be sought by other less intrusive means bearing in mind any collateral intrusion caused.

Collateral Intrusion. Collateral intrusion is where surveillance indirectly intrudes on to the privacy of individuals who are not the direct subject of the surveillance i.e. where innocent bystanders are observed in the course of a covert surveillance operation - children are included within this definition.

Surveillance. Surveillance includes: -

- Monitoring, observing or listening to persons, their movements, their conversations or other activities or communication;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by or with the assistance of a surveillance device.

Surveillance Device. Surveillance Device means any apparatus designed or adapted for use in surveillance.

Civil & Criminal Proceedings. Civil proceedings involve the commission of a civil wrong against another party in breach of common law or statute, where a remedy is sought by that party through a court or tribunal. Criminal proceedings involve the commission of an act where statute or common law defines it as one where the state has determined that prosecution or other proceedings should take place in the criminal courts.

Public Authority. Public Authority means any public authority within the meaning of section 6 of the Human Rights Act 1998 (acts of public authorities) other than a court or tribunal.

Legal privilege. Confidential letters and other communications between a party and their legal advisor in the course of litigation or in the provision of legal advice and assistance are protected from disclosure and use in evidence in proceedings. The protection given to such material will be lost if there are grounds for supposing that the legal advisor is intending to hold or use that information for a criminal purpose. Action which is likely to involve the acquisition of such sensitive material through surveillance requires particular attention by an Authorising Officer and legal advice should be sought if necessary.

Confidential Information. Confidential personal information is information held in confidence concerning an individual whether living or dead. Confidential Journalistic information – includes information acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

Human Rights Act. The Human Rights Act 1998, Article 8 provides protection to an individual's right to privacy.

Communications Data. Communications Data is information relating to the use of a communications service, but does not include the contents of the communication itself.

1. Introduction

- 1.1 On the 25 September 2000 the Regulation of Investigatory Powers Act (RIPA) was brought in to force in England and Wales. The purpose of the Act was to ensure that all public authorities were able to carry out covert surveillance on a statutory basis without breaching The Human Rights Act 1998, Article 8, the right to privacy.
- 1.2 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 consolidates four previous orders relating to covert surveillance and the use or conduct of a covert human intelligence source (CHIS) by public authorities. It sets out which authorities can use such surveillance techniques, on what grounds and who has to authorise their use. This Order is accompanied by two Codes of Practice entitled "*Covert Surveillance and Property Interference*" and "*Covert Human Intelligence Sources*". Intrusive surveillance and property interference cannot be used by Local Authorities. Directed surveillance can be used.
- 1.2 From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 apply. A local authority who wishes to authorise the use of directed surveillance, acquisition of communications data, and/or use of a CHIS under RIPA will need to obtain an order approving the grant (or renewal) of an authorisation or notice from a Justice of the Peace (JP) before it can take effect. This is in addition to the existing authorisation processes under the relevant parts of RIPA.
- 1.3 The Human Rights Act 1998 requires that all actions which may potentially breach an individual's human rights are:
- **Lawful.** Done in accordance with the relevant laws;
 - **Necessary.** In the particular circumstances of each enquiry there is no reasonably available overt method of obtaining the information that is being sought. If there is a reasonably alternative to covert surveillance, then the necessity test will probably not be satisfied.
 - **Proportionate.** Directed surveillance (defined in section 26(2) of RIPA) may involve covertly following people, covertly taking photographs of them or using hidden cameras to record their movements. Section 28(2)(b) of RIPA states that an authorisation for directed surveillance should only be granted if it is proportionate to what is sought to be achieved by carrying it out. A regular criticism in OSC inspection reports is that public authority employees, when completing authorisation forms, do not give enough thought to proportionality, and consequently authorisations are granted where the impact on the privacy of the target is disproportionate to the seriousness of the offence. The Code of Practice states that 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 target 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.
- 1.4 Failure to comply with RIPA does not mean that an authority's actions in relation to surveillance will be unlawful, but it does mean that evidence obtained from surveillance could be inadmissible in court proceedings and jeopardise a successful outcome. Such

action could also be open to challenge as a breach of the Human Rights Act and a claim for damages could be made against the Council.

- 1.5 **Restrictions on the use of RIPA.** The Protection of Freedoms Act 2012 restricts the use of RIPA to conduct that would constitute a criminal offence which punishable by a maximum custodial sentence of six months or more. There are some limited exceptions to this rule, relating to specified criminal offences relating to the underage sale of alcohol and tobacco (Licensing Act 2003). The relevant RIPA tests of necessity and proportionality must still be applied and JP approval obtained.
- 1.6 Haringey Council is committed to implementing the relevant Acts to ensure that an investigation is carried out properly and that the investigation is necessary and proportionate to the alleged offence.
- 1.7 The purpose of this policy is to ensure that the proper procedures are in place in order to carry out covert surveillance; to ensure an individual's right to privacy is not breached; that proper authorisation is obtained for covert surveillance; that the proper procedures have been followed; and that covert surveillance is considered as a last resort having exhausted all other avenues. Haringey Council's policy is implemented and followed in accordance with the Regulation of Investigatory Powers Act 2000 and the Protection of Freedoms Act 2012.
- 1.8 Further information on RIPA can be obtained from the Office of Surveillance Commissioners, or their website www.surveillancecommissioners.gov.uk, which includes the relevant Codes of Practice, together with examples of frequently asked questions for local authorities.
- 1.9 These procedures cover all aspects of RIPA legislation as follows:
 - Section A – general procedures and authorisation processes
 - Section B – communications data
 - Section C – use of Covert Human Intelligence Source (CHIS)
- 1.10 Copies of all relevant application, review, renewal and cancellation forms, together with the application for judicial review form are held on the Council's intranet site. Please contact the Head of Audit and Risk Management if you require forms or access to Communications Data, or to instigate a CHIS.

Section A – General procedures

2. Undertaking Covert Surveillance

2.1 Under Part II of the Regulation of Investigatory Powers Act 2000, public authorities are authorised to undertake Covert Surveillance, which is either Directed Surveillance or the use of a Covert Human Intelligence Source.

2.2 Directed Surveillance is defined under Section 26(2) of RIPA 2000, as being covert, must not be intrusive and is undertaken for the following purposes:-

- As a specific investigation or specific operation.
- To obtain private information about a person.
- Otherwise than as an immediate response to events, in circumstances where it would not have been reasonably practical for an authorisation to be obtained.

2.3 Covert Human Intelligence Source (CHIS) is defined under Section 26(8) (a-c) of RIPA, where information is obtained to assist in the investigation of a crime or to prevent a crime, by a CHIS who:

- Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything, which is:
- covertly using a relationship to obtain information or to provide access to any information to another person; or
- covertly disclosing information obtained by the use of such a Relationship, or as a consequence of the existence of such a relationship.

Test purchases will not ordinarily require CHIS authorisation where the relationship between the purchaser and seller is likely to be limited as exemplified in paragraph 2.12 of the Code of Practice on CHIS.

2.4 Members of the public volunteering information as part of their normal civic duties are not regarded as a CHIS.

2.5 The use of material, which is obtained through Covert Surveillance either as a Directed Surveillance investigation/operation or through a CHIS, can be used as evidence at criminal and civil proceedings.

2.6 The use of any such material which is to be submitted as evidence must comply with common law, section 78 of the Police and Criminal Evidence Act 1984, the Human Rights Act 1998, the Protection of Freedoms Act 2012 and other Acts.

2.7 Any material evidence obtained through the course of the surveillance is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigation Act 1996.

2.8 A CHIS will also have his/her identity protected under the relevant legal procedures.

2.9 Haringey Council is unlikely to use a CHIS as part of its normal operational functions. However, the requirements for the use of a CHIS have been included as Section C of these procedures, for reference and information. Should the use of a CHIS be considered, please contact the Head of Audit & Risk Management or the Head of Legal Services in advance.

- 3. Senior Responsible Officer (SRO)**
- 3.1 Part II of RIPA 2000 provides lawful authority for a public authority to carry out surveillance. The 2010 Code of Practice considers that a public authority should appoint a Senior Responsible Officer (SRO). Within local authorities, the SRO should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard and be responsible for:
- the integrity of the process in place within the public authority for the management of CHIS and directed surveillance;
 - compliance with part 2 of the Act and with the codes of practice;
 - engagement with the OSC 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.
- 4. Authorising Officer (AO)**
- 4.1 An AO will be responsible for any surveillance either through an investigation or operation to be carried out, or for the use of a CHIS.
- 4.2 A list of AO's within Haringey is provided at Appendix 1.
- 4.3 An AO must not be involved with the specific investigation or operation.
- 4.4 Before the AO grants authorisation to use a source (CHIS), the AO should consult with the Borough Commander within the Police Force Area, which is the Metropolitan Police, to ensure that no conflict arises within the area of where the CHIS is deployed. Advice must also be sought from the Head of Audit and Risk Management and Head of Legal Services.
- 4.5 It is an AO's responsibility to ensure that the correct most up to date forms have been used and that these forms have been completed appropriately.
- 4.6 It is an AO's responsibility to ensure that the authorisation is necessary and proportionate. The AO must challenge the Officer as to the use of the authorisation, if the AO considers that:
- The circumstances of the investigation do not meet the criteria set out in the Protection of Freedoms Act 2012;
 - The correct procedures have not been followed properly;
 - An alternative method of obtaining the necessary information can be used;
 - A risk assessment has not been properly completed;
 - Insufficient grounds have been made for obtaining information which will include legally privileged material.
- 5. Collateral Intrusion**
- 5.1 The AO must take into account the risk of intrusion into the privacy of persons other than those who are direct subjects of the operational investigation, such as innocent bystanders.
- 5.2 Measures must be taken wherever practical to avoid unnecessary intrusion into the lives of those not directly involved in the operation.

6. Risk Assessment

- 6.1 A Risk Assessment must be undertaken by the AO before authorisation is given in order to conduct the use of a CHIS, in accordance with Haringey's Policy statement on Health & Safety which can be found in Volume 4, section 10 of the Personnel Management Handbook.

7. Health & Safety

- 7.1 Any form of Covert Surveillance, either Directed Surveillance or the use of a CHIS, must be in accordance with Haringey's Policy Statement, which complies with the Health & Safety at Work Act 1974.

8. Procedure on Directed Surveillance

8.1 Granting of an Authorisation

- 8.1.1 When considering a request for Directed Surveillance, the AO must ensure that the authorisation is necessary in accordance with both RIPA section 28(3) (b) and 29(3) (b); and Article 7A of the 2010 Order. Since 1 January 2004, and the enactment of S.I. 2003 (No. 3171), local authorities can only rely on one necessity ground, namely *'for the purpose of preventing or detecting crime or of preventing disorder'*.
- 8.1.2 The AO should consider whether the surveillance falls under RIPA. Consideration needs to be given to the changes introduced by the Protection of Freedoms Act 2012 (see paragraph 8.1.3 below and also to circumstances when guidance indicates that RIPA does not apply. The code of Practice sets out those circumstances when a RIPA authorisation is not required or not appropriate including:
- The use of CCTV cameras and ANPR systems by the Council does not usually require RIPA authorisation as they are generally carrying out overt, rather than covert, surveillance;
 - If surveillance takes place as an immediate response to events, RIPA authorisation would not be required even if the surveillance would generally fall into one of the categories covered by RIPA.
- 8.1.3 The AO must be satisfied that the request also complies with Section 7A which amends the 2010 Order. The following conditions apply:
- Local authorities can only authorise the use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable (whether on summary conviction or indictment) by a maximum term of at least six months imprisonment, or are related to the underage sale of alcohol and tobacco;
 - Local authorities cannot authorise directed surveillance for the purposes of preventing disorder unless this involves a criminal offence punishable by a maximum term of at least six months imprisonment;
 - Local authorities may use directed surveillance in more serious cases as long as other tests are met, i.e. that it is necessary and proportionate and where approval from a JP has been obtained. Examples where the offence being investigated attracts a maximum custodial sentence of six months or more include serious criminal damage, dangerous waste dumping, serious or serial benefit fraud;
 - Local authorities may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco, again where the necessity and proportionality tests are met and approval from a JP has been obtained;
 - Local authorities may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate 'low-level offences' e.g. littering, fly posting, dog control.

8.1.4 The AO must be satisfied that the surveillance is *necessary* and *proportionate* in order for this to be achieved and must state on the authorisation form how and why they are satisfied in each particular case:

- **Necessity.** The AO must be satisfied that there is a necessity to use covert surveillance in the proposed operation. In order to be satisfied, there must be an identifiable offence to prevent or detect *before* an authorisation can be granted; and
- **Proportionality.** An authorisation should demonstrate how an AO 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 (i.e. using a sledgehammer to crack a nut). Proportionality is not only about balancing the effectiveness of covert methods over overt methods, but of explaining why the particular covert method technique or tactic is the least intrusive. It is insufficient to state that the 'seriousness' of the crime/disorder justifies any or every means available. It is equally unacceptable to consider lack of available resources or a potential cost saving as sufficient grounds to use technological solutions which may be more intrusive than human capabilities. The judgement on proportionality can only be reached once all other aspects of an authorisation have been fully considered.

8.1.5 An effective authorisation would make clear that the four elements of proportionality had been fully considered:

- Balancing the size and scope of the operation against the gravity and the extent of the perceived crime/disorder;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- That the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and
- Evidencing what other methods have been considered and why they were not implemented.

8.1.6 Having reviewed the authorisation and concluded that it is an appropriate use of RIPA and the forms have been completed fully, the AO should set out why they are satisfied or why they believe that the use of RIPA is necessary and proportionate. A simple assertion is insufficient.

8.1.7 The AO must give the authorisation in writing. Copies of all the relevant the authorisation forms are attached as Appendices to these procedures notes. Copies of the final approved forms must be sent to the Head of Audit and Risk Management for inclusion on the central record of authorisations.

8.1.8 If an urgent case requires an authorisation, then it need not be in writing. However, as soon as practically possible, the authorisation must be recorded in writing. This needs to be considered in conjunction with the new judicial approval requirements.

8.2 Information to be provided in the application for Authorisation

8.2.1 A written application for authorisation for Directed Surveillance must:

- describe fully the conduct to be authorised (maps and sketches may also be useful in explaining the limits and extent of the surveillance); and
- the purpose of the investigation or operation.

8.2.2 The application must include the following:

- the reasons why the authorisation is sought;
- the grounds of the relevant operation or investigation, i.e. for the purposes of preventing or detecting crime – the relevant criminal act must be identified;
- the reasons why the surveillance is considered both necessary and proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities where known of those to be the subject of surveillance;
- an explanation of the information which is to be obtained as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required for the surveillance or the recommendation of the level of authority required;
- a subsequent record of whether authority was given or refused, by whom and the date and time.

8.2.3 In urgent cases where oral authorisation has been obtained, when the written authorisation is completed this should include the following:

- the reasons why the AO or the officer entitled to act in urgent cases considered the case so urgent, that an oral, instead of a written authorisation was given,
- the reasons why it was not reasonably practical for the application to be considered by an AO.

8.3 Applying for Judicial Approval

8.3.1 From 1 November 2012, an order approving the grant or renewal an authorisation or notice must be obtained from a Justice of the Peace (JP) before the RIPA authorisation can take effect. If the JP is satisfied that the statutory tests have been met and the use of RIPA is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the technique as described in the application.

8.3.2 The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA. The current processes in place whereby the investigating officer assesses necessity and proportionality, completes the relevant forms and obtains approval from an authorising officer are still required.

8.3.3 It is the responsibility of the investigating officer to make the necessary arrangements with the Courts and Tribunal Service. The officer should contact the administration team to arrange a hearing.

8.3.4 The JP must be provided with a copy of the original RIPA authorisation or notice and any supporting documents setting out the case – all information that is relied on for the application must be provided at this point. For communications data requests, the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assess by the JP as part of their consideration.

8.3.5 The original RIPA authorisation or notice should be shown to the JP but will be retained by the Council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal.

8.3.6 The Council will provide the JP with a partially completed judicial application/order form. The order section of the form will be completed by the JP and will be the official record of the JP's decision. The Council will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals. The Council will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider cancellations or internal reviews.

8.4 Arranging a Hearing

8.4.1 It is the responsibility of the investigating officer to arrange a hearing at the magistrate's court. If an 'out of hours' access to a JP is required, then the investigating officer must make arrangements with the relevant Courts' Service legal staff.

8.4.2 In emergency situations, where the police have power to act, they have the ability to authorise activity under RIPA without prior JP approval. Please remember that no RIPA authority is required in immediate response to events or situations where it is not practical to obtain it e.g. where criminal activity is observed during routine duties and officers conceal themselves to observe what is happening.

8.4.3 Where renewals fall outside working hours, or within holiday periods, it is the investigating officer's responsibility to ensure that the renewal is completed ahead of the deadline.

8.5 Attending a Hearing

8.5.1 The hearing is a legal proceeding and therefore officers need to be formally designated to appear, be sworn in and present evidence or information as required by the JP.

8.5.2 The hearing will be in private and heard by a single JP. The JP may have questions of the officer attending to clarify points or require additional assurance on specific matters. It is therefore important that the relevant case investigator is available and attends the hearing.

8.5.3 The Council's Constitution (part 3, Section E, paragraph 5.02) specifies that it will maintain a list of relevant officers who will be designated to attend a hearing under these circumstances.

8.5.4 It is not necessary for the Council's legal services department's officers to attend the judicial approval hearing under RIPA.

8.5.5 The JP will consider whether they are satisfied that the requirements of RIPA and other relevant requirements have been satisfied. They will also consider whether the person granting the authorisation on behalf of the Council was an appropriate designated person within the local authority and the crime thresholds for directed surveillance have been met. The JP may decide to:

- Approve the grant or renewal of an authorisation or notice. The Council may then proceed to use the technique set out in the application; or
- Refuse to approve the grant or renewal of an authorisation or notice. The RIPA authorisation or notice will not take effect and the Council must not proceed to use the technique. The Council might wish to re-apply for approval depending on the reasons for the refusal;
- Refuse to approve the grant or renewal and quash the authorisation or notice. The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least two working days from the date of the refusal in which to make representations.

8.6 Duration of an Authorisation

- 8.6.1 A written authorisation will cease to have effect at the end of the three-month period from when it was obtained.
- 8.6.2 An urgent oral authorisation or written authorisation, which has been obtained in an urgent case, will cease to have effect after 72 hours from when it was obtained.

8.7 Reviews of an Authorisation

- 8.7.1 Regular reviews of the authorisation must be undertaken to assess the need for the surveillance to continue.
- 8.7.2 Reviews must be undertaken in the following time periods:
- ordinary written authorisations - reviews should be undertaken as required by each operation.
 - a review of an oral urgent authorisation must be taken 24 hours after the authorisation was obtained.
- 8.7.3 If the review indicates that the operation is to be changed in any way e.g. the location, subject(s), equipment/resources etc, then the AO must ensure that all questions on the original application, including the necessity and proportionality elements, are answered fully. Please note that JPs are not required to be involved with internal reviews, but if the review indicates that the offence does not meet the threshold, the use of directed surveillance should stop. If a directed surveillance authorisation is already in force, it should be cancelled.
- 8.7.4 Copies of all completed review forms must be sent to the Head of Audit and Risk Management for inclusion on the Council's central record of authorisations.

8.8 Renewals of an Authorisation

- 8.8.1 If an authorisation ceases to have effect, and the AO considers it necessary for the authorisation to continue for the purpose for which it was given, the AO may renew it as follows:
- for an ordinary authorisation, for a period up to three months.
 - for an urgent oral authorisation, for a period up to 72 hours.
- 8.8.2 All applications for renewal of authorisations for Directed Surveillance should include:
- whether this is the first renewal;
 - every occasion on which the authorisation has been renewed previously;
 - significant changes to the information relating to the conduct to be authorised and also the purpose of the investigation or operation;
 - the reasons why it is necessary to continue with the Directed Surveillance;
 - the content and value to the investigation or operation of the information so far obtained by the surveillance and the results of regular reviews of the investigation operation.
- 8.8.3 Any requests for renewals must follow the authorisation processes set out in sections 8.3 – 8.5 above and must include approval by a JP before the renewal takes effect. Authorisations may be renewed more than once and must be recorded as part of the central record of authorisations. Copies of all completed renewal forms and the completed judicial review application form must be sent to the Head of Audit and Risk Management.

- 8.8.4 A renewal form should be completed when applying for renewal of an authorisation. The corresponding completed judicial review application/form must also be provided.
- 8.9 Cancellation of an Authorisation**
- 8.9.1 The AO who granted or last renewed the authorisation must cancel that authorisation, if s/he is satisfied that the surveillance no longer meets the criteria upon which it was authorised. The cancellation process does not require review or approval by a JP.
- 8.9.2 Where the AO is no longer available, this duty will fall on the person who is taking over the role of AO or any other designated AO within the Council.
- 8.9.3 The cancellation of surveillance must be formally completed and a copy sent to the Head of Audit and Risk Management for inclusion on the Council's central record of authorisations.
- 8.10 Stopping Surveillance Activity**
- 8.10.1 As soon as the decision is taken that Directed Surveillance should be discontinued, instruction must be given to all those involved in the specific investigation or specific operation to stop all surveillance of the subject(s).
- 8.10.2 The date and time when an instruction was given to cease surveillance activity must be recorded in the central record of authorisations and the notification of cancellation where relevant.
- 9. Procedure for the use of surveillance equipment**
- 9.1 Any equipment that is to be used in the course of a Covert Operation, either as Directed Surveillance or through the use of CHIS, must be entered on the written application and authorisation for its use must be sought as part of the application.
- 9.2 Equipment used in the course of a Covert Surveillance must be:
- Labelled clearly as to identity individual pieces of equipment and this identity number must be entered onto the authorisation forms;
 - Stored in a secure area;
 - Logged in and logged out, noting the time, date and officer's name and position.
- 9.3 All details must be completed on all authorisation forms if equipment is used, when renewing, reviewing and cancelling authorisations. Forms should contain details of all resources and equipment, including make/model, serial/registration number where applicable.
- 9.4 Any and all documentation relating to the use of equipment will need to be made available if requested by the Lead Officer, Police and/or the OSC.
- 9.5 The use of overt CCTV cameras does not require RIPA authorisation, however directing overt CCTV cameras at a particular target or location as part of a specific and planned operation will require RIPA authorisation.
- 9.6 On occasions, the police will request use of the Council's CCTV cameras to undertake planned operations which require RIPA authorisation. In order to comply with RIPA legislation and ensure that the operation in practice matches the authorisation granted, the Council's CCTV Team must obtain a copy of the police authorised forms which show clearly the boundaries of the operation (location, target etc). In cases where the

operation is extremely confidential, the police should be referred to the Head of Audit and Risk Management who will obtain a copy of the relevant authorisation form and formally advise the CCTV Team of the scope of the authorised operation.

10. Intrusive Surveillance

10.1 Part II of RIPA provides for the authorisation of intrusive surveillance by the police, HM Customs and Excise, the intelligence services, MOD police and the Provost Marshall of the Royal Navy Regulating Branch, Royal Military Police, the Royal Air Force Police and any other public authority added by Order.

10.2 Intrusive surveillance is surveillance undertaken covertly which is carried out in relation to anything taking place on residential premises without the persons consent; or in any private vehicle and must involve the presence of an individual on the premises or in the vehicle, and may be carried out by the means of a surveillance device.

10.3 Local authorities are not included within the list of organisations or individuals entitled to undertake intrusive surveillance, therefore care needs to be taken that intrusive surveillance is not undertaken inadvertently. As Local Authorities are not authorised to undertake Intrusive Surveillance, Haringey Council will not be involved within this area of the Act.

11. Procedure for Monitoring and reviewing RIPA

11.1 Lead Officer

11.1.1 The Head of Audit and Risk Management will be the lead officer for monitoring the implementation of RIPA and the use of the authorisation forms on behalf of the Director of Corporate Resources, the Council's SRO. If AO's or officers completing the forms have any questions, or need any clarification, the Head of Audit and Risk Management should be contacted.

11.1.2 The central record of all authorisations will be retained and maintained by the Head of Audit and Risk Management on behalf of the SRO, the Director of Corporate Resources. An extract of the relevant departmental authorisations will be provided to AO's on a regular basis to ensure that the central record is complete and up to date.

11.1.3 The records will be retained for three years from the ending of the authorisation.

11.1.4 All departments who undertake RIPA will keep their own record of authorisations.

11.2 Reviewing RIPA

11.2.1 The Lead Officer (on behalf of the SRO), Director of Corporate Resources and designated AO's will review the implementation of RIPA and the Council's policy on a regular basis.

12. Procedure for Data Retention

12.1 Retention of authorisation forms

12.1.1 All authorisation forms must be retained for 3 years from the date on which the authorisation was obtained.

12.1.2 Records kept by Haringey Council will be maintained to preserve confidentiality of persons who have provided information either through in the course of their civil duty or if they are a CHIS.

12.1.3 Any material which is handled, stored or destroyed will be subject to the Data Protection Act 1998.

12.2 Confidential Information

12.2.1 Confidential information and information subject to a legal privilege will be subject to section 98 of the 1997 Act. Only the Chief Executive (or a deputy in their unavoidable absence) may authorise covert surveillance likely to involve confidential information.

13. Central Record of Authorisations

13.1 Each department will send to the Lead Officer copies of all authorisations – including reviews, renewals and cancellations – as soon as authorisation has been obtained. The documents should include copies of all relevant JP authorisations for initial applications and renewals.

13.2 Copies of the Authorisations and JP approvals will be kept as part of the Central Record, which will be maintained by the Lead Officer electronically and in hard copy. The Head of Audit and Risk Management will assign a URN to each authorisation received and notify this to the relevant AO.

13.3 These authorisations will be kept under review to ensure the proper procedures are followed and forms are completed.

14. Complaints Handling

14.1 Independent Tribunal

14.1.1 RIPA 2000 also establishes an independent tribunal and this tribunal will be made up of Senior Members of the Judiciary and the Legal Profession and is independent of the government. The tribunal has full powers to investigate and decide any case within its jurisdiction.

14.1.2 If a complaint is therefore received from an individual who has been subject to surveillance or by a member of the public then that person or persons should be referred immediately to the Investigatory Powers Tribunal.

14.1.3 The address for the Investigatory Powers Tribunal is PO Box 33220 London SW1H 9ZQ. The telephone contact number is 0207 035 3711. More details are found on their website: www.ipt-uk.com

14.2 Haringey's Complaints Procedure

14.2.1 Haringey also has an internal process of dealing with a complaint by a member of the public or a person who has been subject to any form of surveillance.

14.2.2 Any complaint that is received will be referred directly to the Lead Officer.

14.2.3 The Lead Officer will inform the Chief Executive and will assist the Chief Executive in the investigation of the complaint.

14.2.4 The time period for completing an investigation from the date of the complaint will be eight weeks.

14.2.5 A full report and the findings of the investigation will be prepared within two weeks of the investigation being completed.

14.2.6 Thereafter a decision will be taken, as to what action should be taken, in line with the Council's Complaints Policy.

15. Training

15.1 All Authorisation Officers must have received appropriate training to cover Part II of RIPA, before they are able to authorise any applications for Covert Surveillance. The Lead Officer for Haringey provides regular training and briefings to Authorised Officers.

16. Data Protection

16.1 This policy governs Directed Surveillance and CHIS under the Regulation of Investigatory Powers Act 2000 (RIPA). However, even where conduct falls outside of this legal framework and this policy, the Data Protection Act 1998 applies in relation to the use and storage of personal and sensitive personal data. In any given case, the Human Rights Act 1998 and the Freedom of Information Act 2000 also applies along with RIPA.

Section B – Communications Data procedures and sample NAFN application form

1. Communications Data

- 1.1 The powers to access communications data are set out in section 21-25 of RIPA 2000. The Regulation of Investigatory Powers (Communications Data) Order 2010 (S.I. 2010/480) also applies which consolidates three previous orders. These powers apply to local authorities. An important change this Order makes is that the Designated Person who considers and records applications for such data must be a “Director, Head of Service, Service Manager or equivalent”.
- 1.2 Integral to the acquisition of communications data under RIPA is the Single Point of Contact (SPoC). The role of the SPoC, whether that is an individual or a group of individuals within the authority, is to enable and maintain effective co-operation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data.
- 1.3 It is a requirement of RIPA that SPoC officers are appropriately trained and all SPoCs are expected to register their details with the Home Office. The purpose of the register of SPoCs is to provide communications service providers with a mechanism to help determine the authenticity of RIPA requirements being placed on public authorities.
- 1.4 The Code of Practice relating to the acquisition and disclosure of communications data was issued in October 2007. This provides guidance on the procedures to be followed when acquisition of communications data takes place under the provisions of RIPA 2000. The code does not relate to the interception of communications, nor to the acquisition or disclosure of the contents of communications which are covered by separate regulations. The Code of Practice provides guidance on:
- Situations where acquiring communications data is considered necessary and proportionate;
 - Grounds on which each public authority can and can't access communications data;
 - When to grant authorisations and when to issue notices;
 - The duration, renewal and cancellation of authorisations and notices;
 - Record keeping;
 - Data protection
- 1.5 Local authorities are restricted to ‘subscriber’ and ‘service use’ data and, even then, only where it is required for the purpose of preventing or detecting crime or preventing disorder. Haringey Council will only use RIPA powers to acquire communications data during the course of its business.
- 1.6 Subscriber information is set out in section 21(4)(c) of RIPA. This relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it. Examples of subscriber data include:
- Subscriber checks (also known as reverse look ups);
 - Subscribers or account holders’ account information, including payment methods;
 - Addresses for installation and billing.

- 1.7 Service use data falls within section 21(4)(b) of RIPA. Examples of service use data include:
- Itemised telephone call records (numbers called);
 - Itemised records of connections to internet services;
 - Information about amounts of data downloaded and/or uploaded;
 - Records of postal items, such as records of registered, recorded or special delivery items.
- 1.8 Haringey Council uses the National Anti-Fraud Network to process all its applications for communications data. Applications for Communications Data may be made to NAFN by authorised Council officers who are registered users of the National Anti Fraud Network (NAFN) via their secure website at www.nafn.gov.uk. If you wish to obtain communications data, please contact the Head of Audit & Risk Management.
- 1.9 Applicants will follow the NAFN online procedure and use their electronic application forms – the forms within these procedure notes are included for guidance purposes to advise applicants as to the nature and content of the required information. An example of part of the NAFN online application form to be completed is contained within these guidance notes for illustration purposes only. **This must not be used outside of the secure NAFN website.**
- 1.10 Applications will be reviewed by the NAFN SPoC and once he/she is satisfied with the application they will notify the appropriate NAFN registered Designated Person within the London Borough Haringey (see Appendix 1 – Communications Data SPoC) electronically. All electronic communication via email should be through GCSX secure email account.
- 1.11 The Designated Person will review the application in accordance with Haringey's procedures and if satisfied it is appropriate will approve it using the NAFN web based system and notify the NAFN SPoC.
- 1.12 From 1 November 2012, an order approving the grant or renewal an authorisation or notice must be obtained from a Justice of the Peace before the RIPA authorisation for Communications Data can take effect. If the JP is satisfied that the statutory tests have been met and the use of RIPA is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the technique as described in the application.
- 1.13 The processes outlined in Section A, paragraphs 8.3 – 8.5, of these procedures must be followed before the application for Communications Data takes effect.
- 1.14 When the judicial approval for the applications has been received, the NAFN SPoC will then obtain the communications data and notify the applicant electronically. NAFN will keep appropriate records of all actions for audit by the IOCCO.
- 1.15 Once completed the Applicant will forward a 'pdf' copy of the completed application and approval documents, including the judicial approval, to the Head of Audit & Risk Management and the relevant Designated Person for their records.
- 1.16 The new data access provisions are subject to a statutory code of practice. The code of practice sets out in more detail the application process. For example, it requires in writing:
- The reason why obtaining the requested data is considered to be necessary;

- An explanation of why obtaining the data constitutes conduct proportionate to what it seeks to achieve; and
- Specifying the individual to whom the data relates and the exact data that is required.

- 1.17 In exceptional circumstances, an urgent grant of a notice or authorisation may be given orally. Haringey Council does not currently use oral authorisations, but the legislation does allow for this process. Particular care must be given to the use of the urgent oral process, especially as the judicial approval process still needs to be completed and approval obtained. The authorisation must be completed in writing as soon as practicable after the making of the decision.
- 1.18 Proper records must be maintained and this should include any errors made in either the granting of an authorisation, the giving of a notice, or as a consequence of complying with the notice or authorisation.
- 1.19 It is recommended best practice that the original copy of the communications data obtained is held securely by the SPoC. This will ensure that, should any legal action be required, the original – unmarked – communications data can be submitted as evidence. Copies of the communications data received should be provided to the applicant. The actions taken should be recorded on the SPoC log to create an accurate audit trail.
- 1.20 Errors in the use of communications data must be reported to the ICCO. Guidance on errors and those which must be reported to the IOCCO are contained within the code of practice. Reportable errors must be brought to the attention of IOCCO within 5 working days of being discovered. The form is contained within the guidance notes. An error can only occur after a designated person:
- has granted an authorisation and the acquisition of data has been initiated, or
 - has given notice and the notice has been served on a CSP in writing, electronically or orally.

**NAFN website application form – illustration example only (not to be used
outside the secure NAFN website)
Application for Communications Data
Part I Chapter II of the Regulation of Investigatory Powers Act 2000)
London Borough of Haringey**

User:
Department:

<i>The Applicant</i>	
Applicant name	
Rank/Number	NAFN user
Division/department	
Telephone Contact Number	
e-mail address	
Mobile Contact Number	
Fax Number	

This application form is to be used for communications data in respect of either:

- Communication service users 21(4)(c) (Subscriber/account information)
- Use of communications services 21(4)(b) (Billings etc)

This data is necessary for the following primary purpose as specified in 'The Regulation of Investigatory Powers Act 2000'

For the prevention and detection of crime or preventing disorder S22 (2)(b)

Is this the first application to access communications data in respect of this operation/investigation?

Yes
 No

Information about the operation
Please supply an operation name or reference

Please select operation name or reference from the list or

(select an operation)

Enter an operation name or reference

? NECESSITY

State the nature of the investigation or operation and how it relates to the selected statutory purpose

Give a short explanation of the investigation (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together



Please select the service/data required

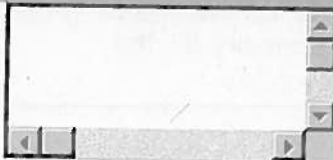
Application data type:

(please select an item)



? COMMUNICATIONS DATA

Describe the communications data required



»Next

Section C – CHIS procedures

1. Procedure for Covert Human Intelligence Source (CHIS)
 - 1.1 Consultation prior to using a CHIS
 - 1.1.1 Although the use of a CHIS is permitted under the Act, caution needs to be exercised by the Council when consideration is being given to the use of a CHIS. Consultation *must* be undertaken with the Head of Audit and Risk Management and Head of Legal Services at the earliest opportunity if the use of a CHIS is contemplated. Specialist training will be required for all relevant officers prior to the use of a CHIS. Consideration of whether the information required could be obtained by other means should be a priority.
 - 1.2 Granting of an Authorisation
 - 1.2.1 Under Part II of RIPA 2000, Haringey is provided with lawful authority under that act to obtain authorisation to use a Covert Human Intelligence Source (CHIS) to assist in the investigation of an operation to detect or prevent a crime.
 - 1.2.2 When an AO considers a request to use a CHIS, for a specific operation or investigation, the AO must believe that the authorisation is necessary for the purpose of preventing and detecting crime, or of preventing disorder.
 - 1.2.3 When undertaking an operation with a CHIS, Haringey Council will be subject to Article 8 of the European Convention of Human Rights 1998. If no lawful authorisation is obtained, then this will be in contravention of Article 8 of the Human Rights Act 1998.
 - 1.2.4 When obtaining an authorisation, the AO must ensure that the authorised use or conduct of the CHIS is a justifiable interference with an individual's rights under Article 8.
 - 1.2.5 The AO must balance the intrusiveness of the use of the CHIS against those being investigated and others who may be affected by the use of a CHIS in all circumstances.
 - 1.2.6 The AO must believe that use of a CHIS is necessary and proportionate and must give the authorisation in writing.
 - 1.2.7 The approval processes for CHIS must include obtaining judicial approval for their use. The application processes outlined at Section A, paragraphs 8.3 – 8.5, of these procedures must be followed before the approval takes effect.
 - 1.2.8 If an urgent case requires an authorisation, then at that time the authorisation is not required to be in writing. However, as soon as practically possible the authorisation must be recorded in writing. Particular care must be given to the use of the urgent oral process, especially as the judicial approval process still needs to be completed and approval obtained. The authorisation must be completed in writing as soon as practicable after the making of the decision.

1.3 Information to be provided in the application for Authorisation

1.3.1 A written application for authorisation for the use of a CHIS must include the following:

- name of the authority;
- name, department, address, contact details of the Applicant;
- the name of the Investigation/Operation if applicable;
- the name and position of the AO;
- the grounds the action is necessary;
- why the use or conduct of a CHIS is necessary;
- why the authorised conduct or use of such a source is proportionate to what it seeks to achieve;
- the purpose of the investigation or operation that the CHIS will be deployed to and identities of the CHIS;
- specific details of the investigation/operation, identities of those to be the subject of surveillance;
- details of what the CHIS Source will be tasked to do;
- details of the risk assessment i.e. security and welfare of source;
- any collateral intrusion;
- any confidential information;
- details of the start date and time of the investigation/operation;
- applicants signature and position;
- AO's comments and signature;
- date of first review and subsequent reviews; and
- confidential information authorisation.

1.3.2 In urgent cases where oral authorisation has been obtained, when the written authorisation is completed this should include the following:

- the reasons why the authorisation is urgent;
- a statement by the AO's, as to why it considered the application was urgent;
- the reasons why it was not reasonably practical for the application to be considered by an AO.

1.4 Duration of an Authorisation

1.4.1 A written authorisation which has been granted by an AO for the use of a CHIS will cease to have effect at the end of a 12-month period from the day that it took effect.

1.4.2 An urgent oral authorisation or written authorisation which has been obtained in an urgent case, will cease to have effect after 72 hours beginning with the time when the authorisation was granted or renewed.

1.5 Reviews of an Authorisation

1.5.1 Regular reviews of the authorisation must be undertaken to assess the need for the surveillance to continue.

1.5.2 Reviews must be undertaken in the following time periods:

- ordinary written authorisations - reviews should be undertaken as required by each operation. A review date should be decided by the

Authorising Officer and recorded on the form when authorisation is agreed.

- a review of an oral urgent authorisation must be taken 24 hours after the authorisation was obtained.

1.5.3 The review must include:

- summary of the investigation/operation to date;
- details as to why it is necessary and proportionate to continue with the use of a CHIS to what is sought to be achieved;
- any details of collateral intrusion and the likelihood of any further intrusions;
- details of any confidential information acquired or likely to be acquired;
- details of the review of the Health & Safety risk assessment;
- review officer's comments, as to whether the use/conduct should continue;
- AO's statement as to whether or not the use of the CHIS should continue.

1.6 Renewal of an Authorisation

1.6.1 If an authorisation would cease to have effect, and the AO considers it necessary for the authorisation to continue for the purpose for which it was given, the AO may renew it as follows:

- for an ordinary authorisation, renewed for a period up to three months;
- for an urgent oral authorisation, renewal for a period up to 72 hours.

1.6.2 All applications for renewal of authorisations for the use of CHIS's should include:

- whether this is the first renewal;
- every occasion on which the authorisation has been renewed previously;
- significant changes to the information relating to the conduct to be authorised and also the purpose of the investigation or operation;
- the reasons why it is necessary and proportionate to continue with the use of the CHIS;
- details of the use of the CHIS, since the grant of authorisation/renewal;
- the task given to the CHIS during that period and the information obtained from that conduct;
- details of the results of the regular reviews;
- details of the review of the risk assessment;
- AO's comment and statement to the continued or discontinued use of the CHIS.

1.6.3 Authorisations may be renewed more than once and, if necessary, the renewal should be kept recorded as part of the central record of authorisations.

1.6.4 Renewals must be completed in writing and judicial approval must be sought prior to the authorisation taking effect.

1.7 Cancellation of an Authorisation

- 1.7.1 The AO who granted or last renewed the authorisation must cancel that authorisation, if he is satisfied that the use of the CHIS is no longer necessary.
- 1.7.2 An explanation as to the value of the CHIS will need to be included.
- 1.7.3 Where the AO is no longer available, this duty will fall on the person who is taking over the role of AO or another designated AO.
- 1.7.4 The cancellation of the use of a CHIS must be completed in writing.

1.8 Stopping Surveillance Activity

- 1.8.1 As soon as the decision is taken that the use of a CHIS is to be discontinued, instruction must be given to all those involved in the specific investigation or specific operation.
- 1.8.2 The date and time when an instruction was given of the ceasing of the use of a CHIS must be recorded in the central record of authorisations and the notification of cancellation where relevant.

1.9 Managing a CHIS

- 1.9.1 Provision is made in s29 of RIPA for a CHIS to be carefully managed.
- 1.9.2 An officer within the Council, following authorisation, is to be tasked with the day to day running of the CHIS, and must;
- keep in regular contact with the CHIS;
 - give them their tasks and monitor progress accordingly; and
 - keep and maintain confidential records about the CHIS.
- 1.9.3 A separate officer is to be appointed within the department to oversee the use made of the CHIS and the Officer with the day to day responsibility of the CHIS.
- 1.9.4 A risk assessment must be carried out in relation to what issues could be facing the security and welfare of a CHIS in relation to what they are to be tasked to do. This should take place before any authorisation is granted and at any renewal, review and cancellation.
- 1.9.5 Special safeguards are in place for vulnerable individuals or juveniles. The first is someone who is or may be in need of community care because of disability, age or illness and may need protecting from exploitation. They should only be used as sources in exceptional cases. The second is a young person under 18. For those under 16, they cannot be used as a source against their parents or anyone with parental responsibility for them. Juveniles can only be authorised as sources for ONE month. For both vulnerable individuals, and juvenile sources, the Head of Service, or Director in their absence, must give authorisation.

APPENDIX 1

AUTHORISING AND SPoC OFFICERS FOR HARINGEY
COUNCIL

Department	Officer's Name/Position	Tel No	Designation
Chief Executive	Nick Walkley Chief Executive	0208 489 2648	Authorising Officer – <i>confidential information only</i>
Corporate Resources	Julie Parker Director of Corporate Resources	0208 489 2688	Authorising Officer (Senior Responsible Officer)
Corporate Resources	Kevin Bartle Assistant Director Finance	0208 489 5972	Authorising Officer
People, Organisation and Development	Stuart Young Assistant Chief Executive	0208 489 3174	Authorising Officer
Place and Sustainability	Lyn Garner Director of Place & Sustainability	0208 489 4523	Authorising Officer
Place and Sustainability	Stephen McDonnell Deputy Director of Place & Sustainability	0208 489 2485	Authorising Officer
Place and Sustainability	Hazel Simmonds Interim Head of Community Safety	0208 489 5458	Authorising Officer
Children and Young People's Service	Libby Blake Director of Children and Young People's Service	0208 489 3206	Authorising Officer
Adults and Housing Services	Mun Thong Phung Director of Adults and Housing Services	0208 489 5919	Authorising Officer
Public Health	Jeanelle de Gruchy Director of Public Health	0208 489 2828	Authorising Officer
Place and Sustainability	Robert Curtis Group Manager, Environmental Crime	0208 489 5583	Communications Data – SPOC