LONDON BOROUGH OF EALING

REGULATION OF INVESTIGATORY POWERS ACT 2000

CORPORATE POLICY AND PROCEDURE

Title	**Regulation of Investigatory Powers Act 2000**
Owner	**Legal Services**
Responsible Officer	**Helen Harris**
Issue Date	
Approved	
Revision Date	**JANUARY 2024**

After the Review date has expired this document may not be up to date so please contact the document owner to check the status after the renew date above.
If you would like help to understand this document or would like it in another format please contact Ealing Council RIPA Legal adviser Ms H. Zeb at zebH@ealing,gov.uk.

CONTENTS

APPENDIX 1: LIST OF AUTHORISING OFFICERS

APPENDIX 2: RIPA "A" AUTHORISATION FORMS
DIRECTED SURVEILLANCE

Form A 1 Application for authority for directed surveillance
Form A 2 Review of Directed Surveillance Authority
Form A 3 Cancellation of Directed Surveillance Authority
Form A 4 Renewal of directed surveillance

APPENDIX 3: RIPA "B" AUTHORISATION FORMS
COVERT HUMAN INTELLIGENCE SOURCES

Form B 1 Application for Authority for conduct and use of CHIS
Form B 2 Review of conduct and use of a CHIS
Form B 3 Cancellation of conduct and use of a CHIS
Form B 4 Renewal of conduct and use of a CHIS

APPENDIX 4: Non -RIPA AUTHORISATION FORM

INTRODUCTION

Everyone has a fundamental right to privacy. This means a right not to be watched, have your emails opened or have your personal space invaded. This right is contained in Article 8 of the European Convention on Human Rights:
"Everyone has the right to respect for his private and family life, his home and his correspondence".
There are times however when the London Borough of Ealing ("the Council") can interfere with this right, provided it has a good reason and follows the proper procedures. Accordingly, the council may interfere with a person's right to privacy, if such interference is in accordance with the law; necessary (as defined in this document); and proportionate.

The Councils use of RIPA is overseen by an independent regulatory body known as the Investigatory Powers Commissioner's Office, where further information about RIPA is also available: - https://www.ipco.org.uk/

This policy should be considered as supplementary to:

(i) Regulation of Investigatory Powers Act 2000
http://www.legislation.gov.uk/ukpga/2000/23/contents

(ii) Home Office guidance on the judicial approval process for RIPA and the crime threshold for directed surveillance.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

(iii) Covert Surveillance and Property Interference Code of Practice – Updated 13 December 2022 (August 2018)
CHIS Code (publishing.service.gov.uk)

(iv) Home Office Covert Human Intelligence Sources – Updated 13 December 2022 (August 2018) CHIS Code draft formatted (publishing.service.gov.uk)

(v) IPCO Guidance – July 2016
https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf

(vi) Article 8 Human Rights Act 1988
https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7

This policy document sets out how the council will comply with Part II of the Regulation of Investigatory Powers Act 2000 (RIPA).

1. POLICY OVERVIEW

1.1 There are three areas that require a RIPA authorisation:

1) Directed Surveillance;
2) Covert Human Intelligence Sources (CHIS);
3) Requests for Communications Data.

Covert surveillance should be used rarely and in exceptional circumstances.

1.2 There should be an audit trail of all RIPA authorisations, reviews, renewals, cancellations and rejections.

1.3 At no time should the Council undertake any surveillance that interferes with any private property such as a dwelling or a private vehicle.

1.4 Directly employed Council staff and external agencies working for the Council are covered by RIPA for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's Authorised Officers.

1.5 In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlap with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 2018 and its Codes of Practice.

1.6 Under normal circumstances, the Council's e-mail and Internet policies should be used, as any surveillance is likely to be more relevant under the contract of employment terms as opposed to RIPA.

2. The Law and how it is to be applied

2.1 The Regulation of Investigatory Powers Act 2000 (RIPA) came into effect in September 2000. RIPA sets out a regulatory framework for the use of covert surveillance techniques by public authorities. If such activities are conducted by council officers then RIPA regulates them in a manner which is compatible with the European Convention on Human Rights (ECHR), particularly Article 8 (the right to respect for private and family life).

2.2 Sections 37 and 38 of the Protection of Freedoms Act 2012 (the Act) came into force on 1 November 2012. Under the Act, local authority authorisations and notices for the use of particular covert techniques (direct surveillance, CHIS and the acquisition of communications data) can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

2.3 In addition amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of 6 months or more or criminal offences relating to the underage sale of alcohol or tobacco.

2.4 Investigations undertaken by Council Enforcement Officers will also from time to time rely upon the use or conduct of a Covert Human Intelligence Source ("CHIS"). This is defined as a person who establishes or maintains a personal relationship or other relationship with a person in order to covertly obtain or disclose information. Although a CHIS can, in law, be either a juvenile or a vulnerable individual, the Council's Policy is that such persons will not be used as CHIS.

2.5 Again, prior to a CHIS being used, RIPA provides that the use must be authorised, and the CHIS can only be used where it is for the purpose of preventing or detecting crime or of preventing disorder. The authorisation ensures that the use of the CHIS is both necessary and proportionate as well as limiting any potential collateral intrusion.

2.6 Article 8 of the European Convention on Human Rights provides that everyone has the right to respect for his private and family life, his home and his correspondence. That right is a qualified right and is not an absolute one. Accordingly, the Council may, in certain circumstances, interfere in the citizen's right mentioned above, if such interference is: -

(a) in accordance with the law;

(a) necessary; and

(b) proportionate.

3. Necessity and Proportionality

3.1 Obtaining a RIPA authorisation will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. It must be necessary for the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. It must also be shown the reasons why the requested activity is necessary in the circumstances of that particular case. Can you achieve the same end result without the surveillance?

3.2 If similar objectives could be achieved by methods other than covert surveillance, then those methods should be used unless it can be justified why they cannot be used.

3.3 Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the subject 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 excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. The interference with the person's right should be no greater than that which is required to meet the aim and objectives.

3.4 The onus is on the Authorising Officer to ensure that the surveillance meets the tests of necessity and proportionality.

3.5 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:

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

3.6 It is important that the staff involved in the surveillance and the Line Manager manage the enquiry and operation and evaluate constantly the need for the activity to continue.

4. Types of Surveillance

4.1 Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained

Surveillance can be **overt** or **overt**.

Overt Surveillance

4.2 Most of the surveillance carried out by the Council will be done overtly- there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about council duties openly for instance an Environmental Health Officer carrying out an inspection of premises to ensure compliance with legislation.

4.3 Similarly surveillance will be overt if the subject has been told it will happen for instance if a noise maker is warned advisably in writing that noise levels will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions and the licensee is told that officers may visit without notice or identifying themselves to the business to check that the conditions are being met.

Covert Surveillance:

4.4 Covert Surveillance is defined in Section 26 (9) (a) RIPA:

"Surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place".

4.5 If activities are open and not hidden from the persons subject to surveillance such as Officers conducting Council business openly, e.g. a market inspector walking through markets, the RIPA framework does not apply because that is "Overt Surveillance". Equally, if you tell the subject that surveillance will be taking place, the surveillance is overt. This would happen, for example, where you warn a noisemaker that noise will be recorded if it continues. RIPA does not regulate Overt Surveillance. Remember it is the Council's responsibilities to ensure that whatever action is taken is compliant with the Human Rights Act and is a necessary and proportionate response to the issue being dealt with.

4.6 The installation of CCTV camera as for the purposes of generally observing activity in a particular area is not surveillance which requires Authorisation as members of the public are aware that such systems are in use for their own protection and to prevent crime.

4.7 An authorisation maybe required if a CCTV camera is to be used for surveillance as part of a specific investigation or operation otherwise than as an immediate reaction to events. In such circumstances either the council or the police will need to obtain the necessary authorisation. If an authorisation is given by the police, then a record of the authorisation will be kept ensuring any surveillance is within its terms.

4.8 Part II of RIPA applies to the following conduct:

- **Directed Surveillance**
- **Intrusive Surveillance; and**
- **The conduct and use of covert human intelligence sources (CHIS)**

Directed surveillance: (Section 26(2) RIPA)
4.9 Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it 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);
- it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

4.10 Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

4.11 By way of examples where directed surveillance is conducted by the council include monitoring of noise complaints; monitoring of benefit claimants who have not declared that they are working/living with a partner etc.

Immediate response to events
4.12 There may be occasions when officers come across events unfolding which were not pre planned which then requires them to carry out some form of observation. This will not amount to Directed Surveillance. However, it will amount to surveillance outside of RIPA and must still be necessary and proportionate and take account of the intrusion issues. Officers must not abuse the process and be prepared to explain their decisions in court should it be necessary. It is important when conducting surveillance in these circumstances that officers still understand that they have obligations to ensure that their actions are Human Rights Act compliant and are therefore necessary and proportionate and take account of the intrusion issues. Therefore, they should document their decisions, what took place, and what evidence or information was obtained.

Recording of telephone conversations

4.13 The recording of telephone conversations connected to criminal investigations outside of the Councils monitoring at work policy for its own equipment falls under RIPA. Where one party to the communication consents to the interception, it may be authorised in accordance with section 46 of the Investigatory Powers Act 2016. In such cases, the interception is treated as directed surveillance.

4.14 There may be occasions where this is required such as a witness who has text or voicemail evidence on their mobile telephone and we require to examine the phone.

Intrusive surveillance:
4.15 Local Authorities cannot conduct intrusive surveillance as regulated by the RIPA 2000.

4.16 Intrusive surveillance is defined in section 26(3) of the 2000 Act as 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.

4.17 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

4.18 Local authorities cannot authorize property interference Entry on or interference with property or with wireless telegraphy as regulated by the Police Act 1997, the Intelligence Services Act 1994 and in certain respects the Investigatory Powers Act 2016.

5. Covert Human Intelligence Source (CHIS)- S26(8) RIPA

5.1 A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as sources. However, it is possible that members of the public, whom repeatedly supply information to Council staff on either one particular subject or investigation or a number of investigations, may become a CHIS. It is important that Council staff make the necessary enquiries of the person reporting the information to ascertain how the information is being obtained. This will not only assist with evaluating the information but will determine if the person is establishing or maintaining a relationship with a third person to obtain the information, and then provide it to the Council staff. If this is the case, the person is likely to be acting as a CHIS and there is a potential duty of care to the individual which a duly authorised CHIS would take account of. Therefore, Council staff should ensure that they are aware of when a person is potentially a CHIS by reading the below sections. If further advice is required contact the RIPA Legal Adviser.

5.2 Under section 26(8) of the 2000 Act a person is a source if:

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

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

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

5.3 By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

5.4 By virtue of section 26(9) (c) of the 2000 Act a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

5.5 Conduct and Use of a Source
The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

5.6 The **conduct of a source** is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

5.7 The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfil whatever tasks are given to them or which is incidental to it. **The Use and Conduct require separate consideration before authorisation.**

5.8 When completing applications for the use of a CHIS you are stating who the CHIS is, what they can do and for which purpose

5.9 When determining whether a CHIS authorisation is required consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

5.10 Management of Sources
Within the provisions there must be;

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare **(Handler)**

(b) at all times there will be another person who will have general oversight of the use made of the source **(Controller)**

(c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

The **Handler** will have day to day responsibility for:

- dealing with the source on behalf of the authority concerned;
- directing the day to day activities of the source;

- recording the information supplied by the source; and

- monitoring the source's security and welfare;

The Controller will be responsible for the general oversight of the use of the source.

Tasking
5.11 Tasking is the assignment given to the source by the Handler or Controller by, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

5.12 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

5.13 Should a CHIS authority be required all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS Codes of Practice

5.14 Security Welfare and Confidentiality
The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

5.15 The confidentiality of the CHIS is paramount, and consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in court.

CHIS and Test Purchases
5.16 Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would **not** normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

5.17 By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a

CHIS and directed surveillance. However, both directed surveillance and CHIS application forms will need to be completed and authorisation obtained. The forms should also be cross referenced.

CHIS and ANTI-SOCIAL BEHAVIOUR

5.18 Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Making Use of CHIS Intelligence Data

5.19 Material obtained from a source may be used as evidence in criminal proceedings. Furthermore, the product obtained by a source described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996. There are also well-established legal procedures that will protect the identity of a source from disclosure in such circumstances. Information obtained from a CHIS must be processed in the same way the product of a Directed Surveillance operation is handled and stored. Access to the information must be restricted and the confidentiality of the CHIS maintained.

Record Management for CHIS

5.20 All original surveillance authorisation (whether authorised or refused), Review, Renewal and Cancellation documents will be forwarded to the RIPA Legal Advisor. The RIPA Legal Advisor will be responsible for maintaining the Central Record of Authorisations and will ensure that all records are held securely with no unauthorised access. The only persons who will have access to these documents will be the RIPA Legal Advisor and the Senior Responsible Officer.

6. Exceptions

6.1 General observation forms part of the duties of the Council and is not usually regulated by RIPA. For example, trading standards officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

7. Examples of Different Types of Surveillance

Type of Surveillance	Examples	Authorisation Required
Overt	• Police Officer or Parks Warden on patrol • Signposted Town Centre CCTV cameras (in normal use)	No
Overt	• Recording noise coming from outside the premises after the occupier has been warned in writing that this will occur if the • noise persists.	No
Overt	• Most test purchases (where the officer behaves no differently from a normal member of the public).	No
Overt	• CCTV cameras providing general traffic, crime or public Safety information.	No
Directed	• Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long-term sick from employment.	Yes
Directed	• Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.	No (but only because not permitted)

8. How Can We Use This Intelligence Data?

General Intelligence Data

8.1 The information must be preserved and properly recorded to ensure that it can be adduced as Prosecution evidence without any doubt as to its probity and value. Furthermore, the product of the surveillance described in this code is subject to the

ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996.

8.2 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection & GDPR requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

9. Storage of the Product of Surveillance

9.1 The 'product' of a Directed Surveillance operation, i.e. the surveillance footage obtained through the operation may be used in as evidence in criminal proceedings. The code of practice issued under the Criminal Procedure and Investigations Act 1996 requires that information obtained during the course of a criminal investigation that may be relevant to the investigation is recorded and retained.

9.2 Departments making use of Directed Surveillance operations must ensure procedures are in place for the secure handling, storage and subsequent destruction of the product of the surveillance.

10. The Acquisition of Communications Data

What is Communications Data?
10.1 Communication data means any traffic or any information that is or has been sent by over a telecommunications system or postal system, together with information about the use of the system made by any person. It is the 'who', 'when' and 'where' of communication, but not the content, not what was said or written.

10.2 The acquisition of communications data under RIPA will be a justifiable only if it is both necessary and proportionate that the conduct being authorised or required take place.

10.3 The Council is only permitted access to under Section 21(4)(b) and (c) of RIPA:

- Service user information; and
- Subscriber information.

Examples of service user information include:

- itemised telephone call records (numbers called);
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the connection, disconnection and reconnection of services;

- information about the provision and use of forwarding/redirection services (by postal and telecommunications service providers);
- information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services;
- information about selection of preferential numbers or discount calls;
- records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Examples of subscriber information include:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 012 345 6789?", "who is the account holder of e-mail account xyz@xyz.anyisp.co.uk?" or "who is entitled to post to web space www.xyz.anyisp.co.uk?";
- subscribers or account holders' account information, including payment method(s) and any services to which the subscriber or account holder is allocated or has subscribed;
- addresses for installation and billing;
- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed).

Procedure

10.4 There are two possible ways of acquiring Communications Data from telecommunications and postal companies ("Communications Companies").

Acquiring Communications Data as a Council

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

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

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

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

10.8 When seeking communications data advice should be sought from the Chris Rabe-Reactive Fraud Manager Audit & Investigations rabec@ealing.gov.uk . Any requests for communications data will be processed with the approval of the SRO (Helen Harris).

10.7 The Council has a Single Point of Contact (SPoC), identified to the Communications Service Provider to enable them to comply with a notice. The SpoC for

local authority communication data requests under RIPA is NAFN. The contact details are:
Address: NAFN Data and Intelligence Services, Thameside MBC, PO Box 304, Ashton Under Lyne, OL6 OGA.
Telephone Helpline 01613423480.
Email: general@nafn.gov.uk.

11. The RIPA Application and Authorisation Procedures

11.1 Since 1 November 2012 the local authorities use of RIPA requires the following consideration:

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

This crime threshold, as mentioned, is only for Directed Surveillance.

11.2 Application, Review, Renewal and Cancellation Forms
No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

11.3 The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP's approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

11.4 The procedure is as follows;
All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP's approval.
The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete the required section of the application for judicial approval form. Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is

supplementary to and does not replace the need to supply the original RIPA authorisation as well.

11.5 It will then be necessary for the applicant to contact Her Majesty's Courts & Tribunals Service (HMCTS) (within Office hours) to arrange a hearing at the Magistrates' Court, to apply to a JP to grant an order approving the authorisation. The hearing will be in private and heard by a single JP.

11.6 Officers who may present the authorisations will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the RIPA Legal advisor.

11.7 Upon attending the hearing, the officer must present to the JP the partially completed application for judicial approval form, a copy of the RIPA authorisation form, together with any supporting documents setting out the case, and in the case of a renewal the original authorisation form.

11.8 The original RIPA authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Investigatory Powers Commissioners' Officers and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

11.9 The JP will read and consider the RIPA authorisation and the application for judicial approval form. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the authorisation form**. However, the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided**.

11.10 The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition, they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

11.11 The JP may decide to:

Approve the Grant or renewal of an authorisation
The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case.

Refuse to approve the grant or renewal of an authorisation
The RIPA authorisation will not take effect and the local authority may **not** use the technique in that case.

11.12 Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

11.13 For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

11.14 Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the authorisation or renew the authorisation and decides to quash the original authorisation or notice. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform the RIPA Legal Adviser who will consider whether to make any representations.

11.15 Whatever the decision, the JP will record their decision on the order section of the judicial approval form. The court administration will retain a copy of the local authority RIPA authorisation form and the judicial approval form. The officer will retain the original authorisation and a copy of the judicial approval form.

11.16 If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date. The officers are now allowed to undertake the authorised activity.

11.17 The original application and the copy of the judicial approval form should be forwarded to the RIPA legal Adviser to be added to the Central Register and a copy retained by the applicant and by the AO. This will enable the AO to check what was authorised and monitor any reviews and cancellation to determine if any errors occurred and if the objectives were met.

11.18 There is no complaint route for a judicial decision unless it was made in bad faith. If the applicant has any issues they must contact the RIPA Legal adviser for advice. A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal team will decide what action if any should be taken.

11.19 All the relevant forms for authorisation through to cancellation must be in writing using the standard forms which are available from the Intranet site and from the RIPA Legal Adviser, but officers must ensure that the circumstances of each case are accurately recorded on the application form (see Application Process).

11.20 If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective application forms and procedures should be followed and both activities should be considered separately on their own merits.

11.21 An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account,

particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

12. Applications

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

12.1 All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. Where appropriate, the Line Manager will perform an initial quality check of the application and/or legal advice sought from the RIPA legal adviser. Completed application forms are to be initiated by Line Managers to show that the quality check has been completed.

12.2 Applications whether authorised or refused by the Authorising Officer will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations.

12.3 If authorised the applicant will then complete the relevant section of the application for judicial approval form and follow the procedure above by arranging and attending the Magistrates Court to seek a JP's approval. (see procedure above RIPA application and authorisation process)

12.4 Duration of Applications

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Juvenile Sources	4 Months
Renewal	12 months

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire.

13. Reviews

The reviews are dealt with internally by submitting the review form to the Authorising Officer. There is no requirement for a review form to be submitted to a JP.

13.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

13.2 In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However, reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

13.3 Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. If the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

14. Renewal

Should it be necessary to renew a Directed Surveillance or CHIS authorisation this must be approved by a JP.

14.1 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors, which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

14.2 The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer.

14.3 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before deciding to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

14.4 If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

14.5 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

15. Cancellation

The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this

duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

15.1 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations. It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by the RIPA Legal Advisor.

15.2 The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance, if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issue instructions regarding the management and disposal of the images etc.

15.3 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

16. Who Can Grant a RIPA Authorisation

16.1 Officers who are designated "Authorising Officers" may authorise the use of directed surveillance or the use of a CHIS whether on a written application or under the urgency oral procedures.

16.2 Please refer to Appendix 1 for the list of Authorising Officers, to show name, contact number and levels of Authority.

16.3 The Chief Executive Officer or in his absence the Executive Director of Children and Adults Services will authorise cases where confidential information is likely to be gathered or in the case of a juvenile or vulnerable CHIS.

16.4 The Director of Legal and Democratic Services (Senior Responsible Officer) will inform the RIPA Legal Advisor of any changes to the list of Authorising Officers and will amend the policy accordingly. The intranet will also be updated appropriately.

16.5 Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. Without a proper understanding of the authorisation process through the correct chain of command you will not be able to comply with RIPA.

17. Working with/through other agencies

When an outside agency has been instructed on behalf of the Council to undertake any action under RIPA, this Document and the Forms in it must be used (as per normal

procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

17.1 When an outside agency (e.g. Police, HM Revenue & Customs) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record.

17.2 If the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

Local Sensitivities

17.3 Authorising Officers and Applicants should be aware of particular sensitivities in the local community where the directed surveillance is taking place, or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. This should form part of the risk assessment.

17.4 It should be noted that although this is a requirement there is no provision made within the application form for this information. Therefore, applicants should cover this area where they feel it is most appropriate such as when detailing the investigation or proportionality or within the separate risk assessment form. This must be brought to the attention of the Authorising Officer when deciding whether to authorise the activity.

18. Authorising Officers Responsibility

18.1 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable such as where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation the Central Record of authorisations should highlight this and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

18.2 Authorising Officers must treat each case individually on its merits and satisfy themselves that the authorisation is in accordance with the law, **necessary** for the prevention and detection of crime, that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

18.3 The Authorising Officer must believe the surveillance is **proportionate** to what it seeks to achieve, considering the **collateral intrusion** issues, and that the level of the surveillance is appropriate to achieve the objectives. If any equipment such as covert cameras, video cameras is to be used, the Authorising Officer should know the capability of the equipment before authorising its use. This will have an impact on

collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

18.4 Authorising Officers are responsible for determining when reviews of the activity are to take place.
Before authorising surveillance, Authorising Officers should also consider the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

18.5 Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should the Authorised Officer approve any RIPA form unless, and until they are satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed.

18.6 Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the latest Procedures and Guidance from the Investigation Powers Commissioners Office (IPCO).

18.7 Before authorising surveillance/use of CHIS, Authorising Officers must be mindful of this policy, training provided by the council and any other guidance issued from time to time.

18.8 When authorising the conduct or use of a CHIS, Authorising Officers must also be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved; be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment and consider any adverse impact on community confidence that may result from the use or conduct or the information obtained.

18.9 In the absence of the Senior Responsible Officer the Application should be submitted to another Authorising Officer for authorisation. (See list of Authorising Officers - Appendix 1)

19. Collateral Intrusion

Collateral intrusion is an integral part of the decision-making process and should be assessed and considered very carefully by both applicants and Authorising Officers.

19.1 The Revised Codes state Collateral Intrusion is intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation such as neighbours or other members of the subject's family. Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance activity should be carefully considered against the necessity and proportionality criteria

19.2 Intended intrusion could occur if it was necessary to follow a person not committing any offences but by following this person it would lead you to the person who is committing the offences.

19.3 Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

19.4 Prior to and during any authorised RIPA activity, a risk assessment should take place to identify the likely intrusion into the subject and any collateral intrusion. Officers should take continuing precautions to minimise the intrusion where possible. The collateral intrusion, the reason why it is unavoidable and your precautions to minimise it will have to be detailed on any relevant application forms. This will be considered by the Authorising Officer.

19.5 Before authorising surveillance, the Authorising Officer should consider the risk of collateral intrusion detailed on the relevant application forms as it has a direct bearing on the decision regarding proportionality.

19.6 The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but you should weigh up the importance of the activity to be carried out in operational terms on the one hand and the risk of collateral intrusion on the other hand.

20. Unexpected Interference with Third Parties

When you are carrying out covert directed surveillance or using a CHIS, you should inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. It will be appropriate in some circumstances to submit a review form and in other cases the original authorisation may not be sufficient, and consideration should be given to whether a separate authorisation is required.

21. Confidential Information

Confidential information consists of matters subject to Legal Privilege, confidential personal information or confidential journalistic material and applications where there is a likelihood of acquiring such information can only be authorised by the Chief Executive **No authorisation should be authorised if there is any likelihood of obtaining legally privileged material without consulting the Legal Services.**

21.1 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records. Journalistic material is also mentioned in the codes; however, it is highly unlikely that this will be obtained.

21.2 Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency business. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. The reasons for acquiring information of this type must be clearly documented and the specific necessity and proportionality of doing so must be carefully considered. Material which has been identified as confidential personal or confidential constituent information should be retained only where it is necessary and proportionate to do so in accordance with the authorised purpose or where otherwise required by law. It should be securely destroyed when its retention is no longer needed for those purposes.

21.3 Where confidential personal or constituent information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from the RIPA legal adviser before any further dissemination of the material takes place.

21.4 Any case where confidential personal or constituent information is retained, other than for the purpose of destruction, and disseminated should be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and any material which has been retained should be made available to the Commissioner on request so that the Commissioner can consider whether the correct procedures and considerations have been applied.

21.4 The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be alert to anything which may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the SRO before further dissemination takes place;

- Confidential material should not be retained or copied unless it is necessary for specified purpose;

- Confidential material should be disseminated only where an appropriate officer (having sought advice from the SRO) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information;

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

22 Use of CCTV

22.1 The use of the CCTV systems operated by the Council does not normally fall under the RIPA regulations. However, it does fall under the Data Protection Act 2018 and the Councils CCTV policy**.** Should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

22.2 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, either the CCTV staff are to have a copy of the application form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority a copy of the applicant's notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been authorised. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the RIPA Legal Advisor for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

22.3 Operators of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

23 Internet Investigations

23.1 The use of the internet as an investigative method is now becoming routine. However, just because the information being obtained is from the internet staff must still consider all the normal rules and guidance applicable to any type of enquiry conducted within a criminal investigation, such as, the Data Protection Act (DPA), Criminal Procedures Investigations Act (CPIA) and RIPA.

23.2 It is important to be aware that the use of social media in an investigation could, depending on how it is used and the type of information likely to be obtained, constitute covert activity that requires authorisation under RIPA.

23.3 Generally researching "open source" material" (example is material you could view on social media without becoming a friend, subscriber or follower) would not require authorisation, but return visits in order to build up a profile could change the position, and this may constitute directed surveillance depending on the circumstances.

23.4 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained,

an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

23.5 Where someone, such as an employee or member of the public, is tasked by the local authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For Example:
a) An investigator using the internet to engage with a subject of interest at the start of an operaton, in order to ascertain information or facilitate a meeting in person;
b) Directing a member of the public (such as a CHIS) to usetheir own or another internet profile to establish or maintain a relationship with a subject of interest for a cover purpose.
c) joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

23.6 Some websites require a user to register providing personal identifiers such as name and phone number before access to the site will be permitted and therefore a CHIS authorisation will not always be appropriate. Where an investigating officer sets up a false identity for this purpose, this doesn't immediately amount to establishing a relationship and so a CHIS is not required, however you should consider a directed surveillance authorisation if the activity is likely to result in the obtaining of private information. For example:
a) A trading standards officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the designer goods being offered are indeed fake. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed, and a CHIS authorisation is not required.
b) trading standards task a member of the public to purchase goods from a number of websites to obtain the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. This should be covered by a CHIS because of the intention to establish a relationship for covert purposes.

23.7 Additionally where a website or social media account requires minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as "like" or "follow" posted by others online would not in itself amount to forming a relationship. Unless you then enter a website and respond on these terms which leads to further interaction with users and a CHIS should be obtained to engage in any further interaction. For example:
a) An investigating officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of this activity he "follows" a variety of people and entities and "likes" occasional posts without engaging any further. No CHIS is required as no relationship is formed.
b) The investigating officer sends a request to join a closed group known to be set up by a subject of interest connected to an investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group further interaction is required as part of the investigation and so a CHIS

authorisation would be required.

23.8 Officers should not use false personae for instance a false Facebook or twitter handle to disguise their online activities. False personae should not be used for a covert purpose without authorisation.

23.9 In order to determine whether an authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- if the investigation is directed towards and individual or organisation;
- if it is likely to result in obtaining private information about a person or group of people;
- if it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- if the information obtained will be recorded and retained
- If the information is likely to provide an observer with a pattern of lifestyle
- If the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- if the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject;
- If it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

23.10 To ensure that no unauthorised online covert activity takes place within the Council please ensure that legal advice is sought from the RIPA legal adviser. The Home Office Codes of practice on covert surveillance and CHIS contain essential guidance in relation to online covert activity and must be considered.

23.11 When an authorisation has been obtained to utilise a false identity to undertake online surveillance the Authorising Officer must maintain a register of identities utilised alongside the record of who is using the profile and for what purpose. All interaction online should be noted/recorded and be the subject of regular audit by the manager to ensure that it is conducted in accordance with the authorisation. The authorising officer should consider the account of such activity at the time of review or renewal of the authorisation.

24 SURVEILLANCE OUTSIDE of RIPA

24.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can now only grant an authorisation under RIPA where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

24.2 There may be a necessity for the Council to undertake surveillance which does not meet the criteria above to use the RIPA legislation such as in cases of serious disciplinary investigations or anti-social behaviour.

24.3 The Council still must meet its obligations under the Human Rights Act and therefore any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision-making process and the management of such surveillance must be well documented. The IPCO Guidance states that it is prudent to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the SRO.

24.4 The Councils Senior Responsible Officer (SRO) will therefore regularly monitor surveillance outside of RIPA. Before any such surveillance takes place, advice must be sought from the RIPA legal adviser.

24.5 As part of the new process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form should be completed and authorised by an Authorising Officer level only. A copy of the non RIPA surveillance application form can be found on the Intranet appendix 4 of this Policy or is available from the RIPA Legal adviser.

24.6 Non RIPA surveillance also includes staff surveillance which falls outside of RIPA. Any surveillance of staff must be formally recorded on the non-RIPA surveillance Application Form and authorised by an Authorised Officer in consultation with the RIPA Legal Adviser who will report to the SRO. A central record of staff surveillance is also maintained by the SRO.

25 Audit trail

Records maintained in the Department

25.1 The following documents must be retained by the relevant Authorising Officer:

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorised Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorised Officer;
- the Unique Reference Number for the authorisation (URN).

26 Central Register maintained by the Legal Department of the Council

26.1 The RIPA Legal Advisor, Hatoon Zeb will retain a Central Record for a period of at least three years from the ending of the authorisation. The Investigatory Powers

Commissioners Office (IPCO) can audit/review the Council's policies and procedures, and individual authorisations.

As well as the Central Record the RIPA Legal Advisor will also retain:

- the original of each application, review, renewal and cancellation, copy of the judicial approval form, together with any supplementary documentation of the approval given by the Authorising Officer
- a record of the period over which the surveillance has taken place;

26.2 Annual Report to Investigatory Powers Commissioners Office (IPCO)
The Council is required to provide statistics to the IPCO every year in March for the purposes of the IPCO Annual Report. The RIPA Legal Advisor shall be responsible for completing the return and providing the statistics.

27 Storage and Retention of Material

27.1 All material obtained and associated with an application will be subject of the provisions of the Criminal Procedures Investigations Act 1996 (CPIA), Codes of Practice which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances. It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of the Data Protection Act 2018 and or GDPR.

27.2 All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained together with relevant associated paperwork should be held securely and ensure any dissemination of the product takes account of the DPA and is only disclosed to those that can lawfully receive it. The material may only be retained for as long as is necessary, therefor material which will be retained outside of the CPIA provisions (see below) must have some justification to meet the DPA &/ GDPR requirements. If in doubt advice should be sought from the Data Information Governance Manager.

27.3 Extra care needs to be taken if the application and material relates to a CHIS as set out above.

27.4 Material is required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

27.5 Where the accused is convicted, all materials which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

27.6 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

27.7 Departments making use of Directed Surveillance operations must ensure procedures are in place for the secure handling, storage and subsequent destruction of the product of the surveillance. Whilst each department will have its own internal procedure for the handling of evidence, below is a non-exhaustive list of factors which should be considered.

- Details of the product of surveillance must be recorded including the date, time and place the product was obtained and the operation to which it relates.
- The product must be kept in secure storage with access to the product restricted.
- The movements of the product must be recorded. If the product is removed from storage, the time, date and reasons for the movement of the product must be recorded; so too the details of the recipient of the product and the person authorising its removal from storage. Similarly, records must be updated when the product is returned to storage and when the product is destroyed.
- Any product that is deemed to be of no use in proceedings must be destroyed immediately. If the product is used as evidence in proceedings, it must be securely stored and destroyed with the additional evidence in accordance with the department's internal procedures.

28 Training

28.1 There will be an ongoing training programme for Council Officers who will need to be aware of the impact and operating procedures with regards to this legislation. The RIPA Legal Adviser will be required to retain a list of all those officers who have received training and when the training was delivered.

28.2 Authorising Officers must have received formal RIPA training before being allowed to consider applications for surveillance and CHIS.

29 Errors

29.1 An error must be reported if it is a "relevant error", which is defined under section 31(9) of the Investigatory Powers Act 2016 as being any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by the authority with Part II of RIPA. Examples of relevant errors occurring would include circumstances where:

• Surveillance or Covert Human Intelligence Source activity has taken place without lawful authority

• There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Codes.

29.2 All relevant errors made by the Council of which it is aware must be reported to the IPC as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner). Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

29.3 From the point at which the Council identifies that a relevant error may have occurred, it must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the Council must also inform the Commissioner of when it was initially identified that an error may have taken place.

29.4 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days (or as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report should include information on the cause of the error; the amount of surveillance conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence. The Investigatory Powers Commissioner may issue guidance as necessary, including guidance on the format of error reports. The Council must have regard to any guidance on errors issued by the Investigatory Powers Commissioners.

29.5 If the Investigatory Powers Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error, they will inform them. An error is a serious error where it is considered to have caused significant prejudice or harm to the person concerned. In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner will in particular consider:

• The seriousness of the error and its effect on the person concerned

• The extent to which disclosing the error would be contrary to the public interest or prejudicial to:

- national security
- the prevention or detection of serious crime
- the economic well-being of the United Kingdom
- the continued discharge of the functions of any of the security and intelligence services

29.6 Before making his or her decision, the Commissioner will ask the Council to make submissions on the matters concerned, and the Council must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

When informing a person of a serious error, the Commissioner will inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

29.7 This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria but allows it to continue. This would be surveillance outside of RIPA.

30 Reporting to Members

30.1 Quarterly updates of any surveillance activity undertaken by Council staff including joint surveillance and Directed Surveillance using the CCTV system will be compiled by the RIPA Legal Advisor and reported to the SRO to update the Portfolio Holder for Finance and Performance in line with the current advice in the Codes of Practice. Members will review on a yearly basis the policy to assess whether the activity undertaken is in line with this policy.

40. Scrutiny and Tribunal

40.1 Scrutiny will be provided by the Investigatory Powers Commissioners Office (IPCO) The Commissioner will periodically inspect the records and procedures of the Authority to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

40.2 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for enabling him to carry out his functions.

40.3 A tribunal has been established to consider and determine complaints made under RIPA if it is the appropriate forum. Persons aggrieved by conduct, e.g. directed surveillance, can make complaints. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that period.

Complaints can be addressed to the following address

Investigatory Powers Tribunal
PO Box 33220
London
SW1H9ZQ