POLICY & PROCEDURES
on
COVERT SURVEILLANCE
and use of
COVERT HUMAN INTELLIGENCE SOURCES
under the
REGULATION OF INVESTIGATORY POWERS ACT 2000

August 2020

CONTENTS

NOTE:

This Document must be read in conjunction with the:

- Revised Code of Practice for Covert Surveillance and Property Interference, August 2018 ('CS CoP'),- (Intranet- *Regulation of Investigatory Powers Act 2000*)
- Revised Code of Practice for Covert Human Intelligence Sources, August 2018 ('CHIS CoP') -(Intranet- *Regulation of Investigatory Powers Act 2000*)
- Protection of Freedoms Act 2012 – changes to provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) - (Intranet- *Regulation of Investigatory Powers Act 2000*)

And, in respect of CCTV,

- The Home Office Surveillance Camera Code of Practice, June 2013

Copies of this Document, the Application Forms and the Codes of Practice are located on the Intranet/ (Intranet- *Regulation of Investigatory Powers Act 2000*)

LONDON BOROUGH OF HAVERING POLICY & PROCEDURES
- REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

A. Background

The Human Rights Act requires the Council, and organisations working on its behalf, to have respect for the private and family life of citizens. However, in rare cases, it may be necessary for the Council to act covertly in ways that may interfere with an individual's rights.

The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a mechanism for authorising covert surveillance and the use of "covert human intelligence sources" (CHIS). It aims to ensure that any interference with an individual's privacy is **necessary** and **proportionate**, and for the purpose of the protection of both the public interest and the human rights of individuals.

It is important to note that the legislation does not only affect directly employed Council staff. Where external agencies are working for the London Borough of Havering, carrying out the Authority's statutory functions, the Authority remains liable for compliance with its duties. It is essential that all external agencies comply with the regulations, as they are contractually obliged to do so. Therefore, work carried out by agencies on the council's behalf should be properly authorised by one of the Council's designated Authorising Officers.

If the correct procedures are not followed:

- **evidence could be thrown out**
- **a complaint of maladministration could be made to the Ombudsman**
- **the Council could be the subject of an adverse report by the Investigatory Powers Commissioner's Office (IPCO)**
- **a claim could be made leading to the payment of compensation by the Council**
- **there could be adverse publicity which could have a serious impact on the Council's reputation**

B. What RIPA does and doesn't do

RIPA does

- require authorisation of directed surveillance
- prohibit intrusive surveillance
- require authorisation of the conduct and use of a CHIS,
- require safeguards for the use of CHIS.

RIPA does not make unlawful conduct which is otherwise lawful, and it does not prejudice any existing power to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtaining information via the DVLA, or to get information from the Land Registry as to the owner of property.

RIPA does provide valuable legal protection against claims and complaints and therefore **compliance with its requirements and these procedures are mandatory for all services and staff**.

C Procedure

Officers should consider each of these points when starting and conducting an investigation.

1. Ensure complaint is recorded and kept up-to-date on recording system.

2. A full note of evidence must be maintained.

3. Ascertain whether the investigation being conducted is one that will or will not likely involve covert surveillance of any person or which may reveal confidential personal information about anyone. If covert surveillance is likely or intended to result in the acquisition of confidential or legally privileged information, the special rule applies (see below.
   .

4. Ascertain whether a **Covert Human Intelligence Source (CHIS)** is necessary. Apply the special rule if the CHIS is under the age of 18 or is a vulnerable individual or when knowledge of legally privileged or confidential information is likely to be acquired. If the special rule is applied this must be the subject of prior consultation, with the Monitoring Officer or the Deputy Monitoring Officer.

5. Before starting covert surveillance or using CHIS, obtain a number and written authorisation from the relevant officer(s) (see Flow Chart and Forms).

6. Surveillance during an investigation conducted by one of the above people must be authorised by another authorised person.

7. Authorising Officers must not grant or renew authorisations unless satisfied that the requirements are met (see Grounds for Authorisation).

8. An application for authorisation must be made on the relevant form. The forms are available from the intranet – search for 'RIPA'. The relevant forms are:

Surveillance	**CHIS**
Authorisation to **conduct** Directed Surveillance	Authorisation to **conduct** CHIS
Authorisation to **renew** Directed Surveillance	Authorisation to **renew** CHIS
Authorisation to **cancel** Directed Surveillance	Authorisation to **cancel** CHIS
Review of Directed Surveillance Authority	Review of Conduct and Use of a CHIS

9. Urgent cases There is now no power to grant urgent oral authorisations. Written authorisation from a Justice of the Peace is required using the standard procedure.

10. Officers should ensure that the officer granting the authorisation regularly reviews it. Officers should cancel authorisation where surveillance is no longer necessary or proportionate to the investigation in progress.

11. Authorising Officers should ensure that authorisations are renewed and/or cancelled before they expire.

12. The officer responsible for authorisation of the investigation must immediately inform the Public Protection Manager as the Co-ordinating Officer by e-mail of the grant, renewal or cancellation of all authorisations

13. Authorising Officer must ensure that all materials are secured and originals sent to the Public Protection Manager (as the Co-ordinating Officer), and disposal of expired material is timely. Officers are responsible for continuously maintaining RIPA standards.

The following time limits apply to an authorisation:

Type of authorisation	**Expiry Period**
Covert directed surveillance	A maximum of 3 months, reviewed regularly, and timely cancellation when appropriate
CHIS	A maximum of 12 months (4 months if CHIS is under 18), reviewed regularly, and timely cancellation when appropriate

D Types of Surveillance

"Surveillance" includes

- monitoring, observing, listening to persons, their movements, conversations, other activities or communications
- recording anything monitored, observed or listened to in the course of surveillance
- surveillance, by or with, assistance of a surveillance device.

Surveillance can be overt or covert.

Overt Surveillance

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 business openly (e.g. a market inspector walking through Romford Market). An immediate response may be appropriate in certain instances e.g. if an occurrence is witnessed action could follow to see what if anything takes place. Similarly, surveillance will be overt if the subject is aware it will happen (e.g. where a noisemaker is warned that noise will be recorded if the noise continues, or where a licence is issued subject to conditions and the licensee is told that officers may visit without identifying themselves to check that the conditions are being met).

Covert Surveillance

Surveillance is Covert Surveillance if, and only if, it is carried out in a manner calculated to ensure that persons subject to the surveillance are unaware it is taking place. (Section 26(9)(a) of RIPA.)

RIPA regulates two types of covert surveillance (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHISs):

Directed Surveillance

Directed Surveillance is surveillance which

- is covert surveillance; and
- is not intrusive surveillance (see definition below) – **the Council must not carry out intrusive surveillance**.
- is not carried out as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable e.g. spotting something suspicious and continuing to observe it; *[CS CoP 3.32]* and
- it is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). *[CS CoP 2.4 and 3.1]*;

Private information in relation to a person includes any information relating to his/her private or family life. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. RIPA does not apply in situations involving the general monitoring and use of town centre CCTV. These cameras are overt and so cannot generally be used for covert monitoring.

Prolonged surveillance targeted on a single person may very well result in the obtaining of private information. Similarly, although overt town centres CCTV cameras do not normally require authorisation, if the camera is tasked for a specific operation, which involves prolonged surveillance on a particular individual, authorisation may well be required. The way a person runs their business may also reveal information about his or her private life.

Council Officers can carry out "Directed Surveillance" IF, AND ONLY IF, the RIPA authorisation procedures are followed.

Intrusive Surveillance

- is covert
- relates to residential premises and private vehicles; and
- involves the presence of an individual on the premises or in the vehicle; or is carried out by a surveillance device. If a surveillance device is not on the premises or in the vehicle it is not intrusive, unless it consistently provides information of the same quality as if it was on the premises or in the vehicle
- or relates to premises used for the purpose of legal consultations
- can be carried out only by police and other law enforcement agencies

Council Officers must not carry out intrusive surveillance.

Examples of different types of Surveillance

Surveillance will fall into one of four categories:

Type of Surveillance	Examples

Overt	• Uniform Police Officer on patrol. • Signposted Town Centre CCTV Cameras (in normal use) • Recording noise coming from premises after the occupier has been warned that this will occur if the noise persists. • Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert, but may not require authorisation	Hidden CCTV camera focused on a railway bridge which has just been cleared of graffiti, where it is expected that taggers will target the bridge. However if collateral information is likely to be obtained then RIPA authorisation is necessary.
Directed – requires a RIPA authorisation.	• Officers follow an individual over the course of the day, to establish whether he is working when claiming benefit • Test purchases where the officer has a hidden camera recording information which might include information about the private life of a small shop-owner, e.g. the way they run their business.
Intrusive - Council cannot do.	Planting a listening device (bug) in a person's home or in their private motorcar.

Directed and Intrusive Surveillance is subject to the Revised Code of Practice for Covert Surveillance and Property Interference, August 2018 **issued under s 71 of RIPA.**

The Protection of Freedoms Act 2012 introduced new requirements concerning the use of directed surveillance. **Local authorities 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 six months or more or criminal offences relating to the underage sale of alcohol or nicotine products like tobacco. A local authority 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 which may include, for example, littering, dog control and fly-posting**.

However, RIPA does *not* prevent the Council from conducting other investigations, even if covert surveillance techniques are used.

If RIPA does not apply, the Council must follow procedures similar to RIPA and ensure that any surveillance pursues a legitimate aim and is necessary, proportionate and justifiable in all the circumstances of the case. This will ensure compliance with data protection legislation and the Human Rights Act 1998, in particular, Article 8.

Covert surveillance of Social Networking Sites (SNS) and On-line Accounts

Reference should be made to paragraph 288 of the OSC Procedures and Guidance 2016.

The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation.

Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat or persistent viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

The RIPA regime was introduced before the rise of electronic media such as Twitter and Facebook where individuals voluntarily put lots of personal information 'on-line' with varying degrees of public accessibility. Such sites can be a very useful source of research for an investigator. The applicability of RIPA to such information sources is a developing area, but currently the Council will follow the following rules:

a) Casual or occasional checking of an individual's on-line account which is open to all is regarded as akin to walking past a person's house or shop and does not need authorisation under RIPA.

b) Targeted, on-going checking of an 'open' account is effectively the electronic equivalent of carrying out physical surveillance of an individual. While currently there isn't a definitive legal ruling on the issue, in order to prevent possible challenge to any evidence gained in this manner, a RIPA authorisation should be obtained.

c) Accessing an individual's account by becoming that person's 'friend', even if there is no intention to have additional contact, requires a RIPA authorisation.

d) Any access of an account which will involve an on-going dialogue with the targeted individual is forming a relationship with the individual and requires a CHIS authorisation.

See also Appendix C for important Home Office guidance on the use of the internet as a surveillance tool.

Children and Young People's Services

For cases of suspected abuse, directed covert surveillance, may be an appropriate adjunct to ordinary social care practice including family visits. Where it is suspected that abuse amounting to a crime is being carried out, and where no other means can be found to confirm the position, a Multi-Agency Strategy Meeting should be convened, and the decision to recommend covert surveillance should be considered against the tests above, formally recorded, and then passed to an authorising officer in the local authority or the police.

For school admissions, covert surveillance is almost certainly not an option because of the need to identify a criminal offence with a possible 6 month custodial sentence and questions about the proportionately of such actions. Information can be acquired from

parents and carers to demonstrate residence through overt means, such as the production of utility bills, health registrations, mortgage or rent documentation, Council tax records, and membership of libraries, churches, or other local organisations. In cases where a family has broken up, the main residence of the child should be confirmed by court documents.

E. Conduct and Use of a Covert Human Intelligence Sources (CHIS) (e.g. informers, undercover agents)

Who is a CHIS?

Under the 2000 Act, a person is a CHIS 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.

A relationship is established or maintained for a covert purpose if and only if it is conducted in manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

The provisions of RIPA 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.

See also Appendix D for important Home Office guidance on distinguishing between people who volunteer information and the use of informants.

Use of a CHIS

The Council is extremely unlikely to deploy a CHIS and any officer contemplating such a step should consult the Monitoring Officer or Deputy Monitoring Officer within Legal Services.

What must be authorised

The Conduct or Use of CHIS requires authorisation.

- **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
- **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS.

The Council can use a CHIS IF, AND ONLY IF, RIPA procedures are followed.

Juvenile Source

Special safeguards apply to the use or conduct of juvenile sources (those under 18 years old). On no occasion can a child under 16 years of age be authorised to give information against his or her parents *[see CHIS CoP 4.2].* Only the Chief Executive or, (in his/her absence) the person acting as the Head of Paid Service can authorise the use of Juvenile Sources. The duration of the authorisation is **four** months only.

Vulnerable individuals

A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation. A vulnerable individual should only be authorised to act as a source in the most exceptional circumstances. The Chief Executive or, (in his/her absence) the person acting as the Head of Paid Service are the only persons who can authorise the use of a vulnerable person as a CHIS.

Test Purchases

Carrying out test purchases will not normally 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). By contrast, developing a relationship with a person in the shop to obtain information about the sellers suppliers of an illegal product (e.g. illegally imported wild meat) is likely to require authorisation as a CHIS. Similarly, using hidden recording devices to record what is going on in the shop (e.g. a hidden CCTV Camera) may require authorisation as directed surveillance. A combined authorisation can be provided if a CHIS is carrying out directed surveillance.

Noise

Persons who complain about excessive noise, and are asked to keep a noise 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.

However, if the Council serves notice on the owner/occupier of the premises and the source of the noise is a third party, authorisation under RIPA may be required. The investigation may (i) be covert in relation to that third party and (ii) may reveal private information about them.

F. Authorisation

Directed surveillance and the use of a CHIS can be carried out only if authorised, and only within the terms of the authorisation. Appendix A provides a flow chart of process from application to record management.

Authorising Officers:

Authorisations can only be given by Authorising Officers, listed in Appendix B.

Only the Chief Executive or, (in his/her absence) the person acting as the Head of Paid Service can authorise covert surveillance if **legally privileged or confidential information** is likely to be acquired or when a **juvenile or vulnerable person** is to be used as a source.

Authorisation under RIPA is quite separate from delegated authority to act under the Council's Scheme of Delegation and internal directorate Schemes of Management. **RIPA authorisations are for specific investigations only and must be cancelled once the specific surveillance is complete or applied to be reviewed when about to expire if the investigation is continuing.**

The Authorising Officer should not just "sign off" an authorisation, but must give **personal consideration** to the **necessity** and **proportionality** of the proposed action and any **collateral intrusion** which may result, and must personally ensure that the surveillance is reviewed and cancelled.

Application Forms:

Applications for authorisation should be made using standard RIPA forms. Forms seek to ensure that criteria for RIPA are fully considered.

London Borough of Havering currently uses the following Home Office forms (available from the Intranet / *RIPA*)

- Application for Authority for Directed Surveillance
- Application for Renewal of Directed Surveillance Authority
- Cancellation of Directed Surveillance
- Review of Directed Surveillance Authority
- Application for Authority for Conduct and Use of a CHIS
- Application for Renewal of Conduct and Use of a CHIS Authority
- Cancellation of Conduct and Use of a CHIS

- Review of Conduct and Use of a CHIS
- JP approval form

Grounds for Authorisation

See also section 28(3) of the RIPA Act 2000

Directed Surveillance, or the Conduct and Use of a CHIS can be authorised by the Council **only** on the following grounds:

- For the **prevention or detection of crime**

Before seeking authorisation, the applicant is to contact the Public Protection Manager as Co ordinating Officer (x2771) for a Unique Reference Number (URN). Certain information will be required at this stage to be input onto a corporate log of RIPA activities

Assessing the Application Form.

When considering whether to authorise surveillance an Authorising Officer must

- Consider the relevant Code of Practice
- Ensure that the exact nature of the surveillance is fully described so that the Authorising Officer is fully aware of what he/she is being asked to authorise.
- Satisfy him/herself that the authorisation is **necessary** in the circumstances of the particular case on the grounds of the prevention or detection of crime, and also
- Satisfy him/herself that the surveillance is **proportionate** to what it seeks to achieve *[CS CoP 4.6 – 4.7].* In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer will consider other appropriate means of gathering information. In the case of the CHIS, authorisations, (see also CHIS CoP 3.2 – 3.5).

  - Proportionate involves **balancing** 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 **excessive** in the circumstances of the case.
  - The activity will not be proportionate if the information which is sought could reasonably be **obtained by other less intrusive means**. e.g. if the evidence could have been gathered through other methods of investigation, such as unannounced inspections, then these less intrusive and non-covert methods should have been exhausted first.
  - **Proportionate also involves balancing the Human Rights of the subject of the surveillance against the seriousness of the offence under investigation.**

  If there is an alternative practicable means of carrying out the surveillance, which is less intrusive, then the surveillance is neither necessary nor proportionate and should not be authorised.

- Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid collateral intrusion *[see CS CoP 4.11 – 4.16].*
- Set a date for review of the authorisation
- Ensure that the Public Protection Manager is sent the top copy of the authorisation for filing centrally.

Additional Factors when Authorising a CHIS

In addition, when authorising the conduct or use of a CHIS the Authorising Officer must be

- be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved and
- be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS;
- consider the likely degree of intrusion of all those potentially affected.
- consider any adverse impact on community confidence that may result from the use or conduct or the information obtained.
- ensure **records** contain statutory particulars and are not available except on a need to know basis.

Urgent Authorisations

Until April 2013 it was possible in exceptional circumstances to give urgent authorisations orally. This practice is now prohibited by changes introduced by the Protection of Freedoms Act 2012. All authorisations (grants and renewals) have to be made in writing by a Justice of the Peace after completion of the Council's internal process. The Magistrates Court has provisions for contacting an out-of-hours duty magistrate – details are held at Romford Police Station.

Immediate Responses

There are certain events situations which require an immediate response where it would be impracticable to obtain an authorisation. Such surveillance is not deemed to be directed surveillance for the purposes of RIPA. An example would be Council officers needing to covertly observe an activity that they come across during their routine duties.

Duration

The authorisation period for Directed Surveillance is 3 Months and 12 Months for a CHIS (except for a CHIS for a juvenile which is 4 months).

Review and Cancellation

The Authorising Officer must review authorisations frequently, and must cancel an authorisation promptly if he/she become satisfied that the surveillance is no longer required or appropriate. An authorisation must be cancelled in all cases, it cannot be left to expire at the end of the authorisation period. When cancelling the authorisation the Authorising Officer is required to consider whether the surveillance was effective,

necessary, and met its objectives. Cancellations must be made using the cancellation form *[CS CoP 5.22 – 5.24].*

Renewals

Authorisations can be renewed in writing when the authorisation period expires. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.

The renewal will begin on the day when the authorisation would have expired and will last for a further 3 months *[CS CoP 5.18]*. Renewals can no longer be renewed orally in urgent cases and have to be approved by a Justice of the Peace.

G Record maintenance

The Council must keep a detailed record of all authorisations, renewals, and cancellations *[CS CoP Chapter 8]*

Records maintained by Requesting Officer and Centrally

The following documents must be securely retained by the Requesting Officer and originals sent to the Public Protection Manager as the Co Ordinating Officer for recording centrally:

- A copy of the application and a copy of the authorisation 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 Authorising Officer; Reviews can be undertaken earlier in order to gain an understanding of what is working in practice.
- 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 Authorising Officer.
- The date and time when any instruction was given by the Authorising Officer.
- A copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace.

- The Council shall retain records for a period of at least three years (and usually for up to five years) from the ending of the authorisation *[CS CoP 8.2 & 8.5].* The Investigatory Powers Commissioner's Office (IPCO) can review the council's policies and procedures, and individual authorisations. IPCO usually provide notice before an inspection, but can arrive unannounced.

Copies of authorisations, renewals and cancellations are discoverable in legal proceedings. If proper records are not maintained, evidence gathered may be inadmissible.

H. Single Point of Contact (SPOC)

As of 5 January 2004, access to communication data to further investigatory work (in areas like trading standards, environmental health, benefits fraud and planning functions) fell under the RIPA 2000. Each Authority is required to establish a SPOC to interface with the many communication service providers (Telecoms, Internet and Postal companies) who hold this data.

The Council's SPOC is the Public Protection Manager, in collaboration with the National Anti-Fraud Network (NAFN).

I. Oversight

In accordance with recommended best practice, the Council has appointed its Monitoring Officer and Deputy Director of Legal & Governance as the Senior Responsible Officer for the purposes of RIPA. This officer is responsible for,

- the integrity of the process in place within the Council to authorise directed surveillance and the conduct and use of a CHIS;
- compliance with Part II of the 2000 Act,
- and with the relevant codes;
- reporting any errors in complying with the requirements of RIPA to the IPCO (in accordance with section 235(6) of the Investigatory Powers Act 2016) as soon as reasonably practicable, and no later than ten working days;
- engagement with the Commissioners and inspectors when they conduct their inspections;
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner and
- ensuring that all *authorising officers* are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners

The Senior Responsible Officer will:

- Report to the Council's Governance Committee at least once a year on the use of RIPA and reviewing the Council's policy
- Report to the Leader and the Lead Member and oneSource Management (on use under functions delegated to oneSource) at least once a year to ensure that it is being used consistently with this policy and these procedures and that the policy and procedures remain fit for purpose.

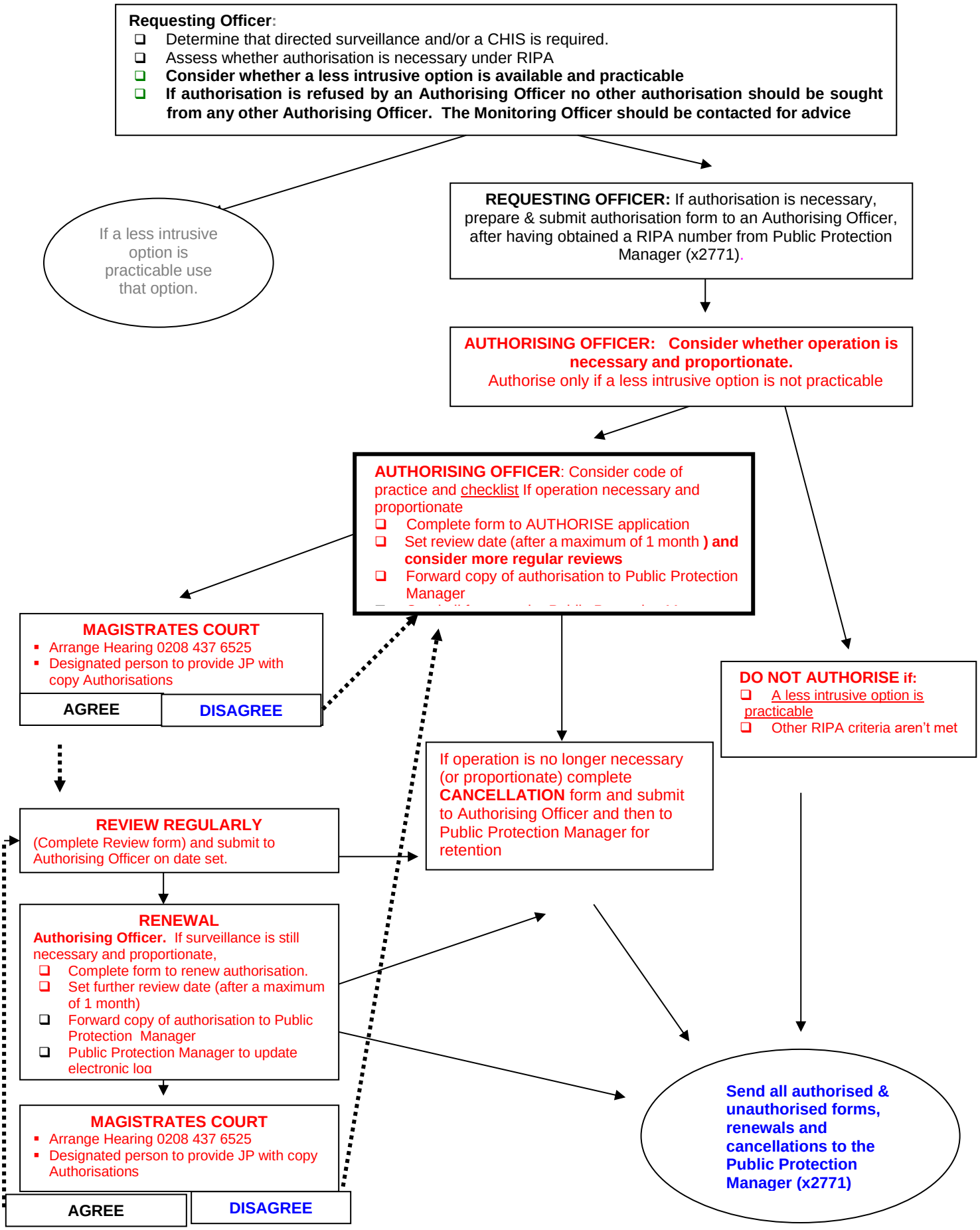
J. Training

- Training is required and mandatory for all Council Authorising Officers and staff involved with any aspect of investigation and surveillance.
- Home office accredited training is mandatory for the Council's SPOCs

- It is also the responsibility of managers to ensure that appropriate staff receive the appropriate training and guidance on RIPA.

Further information and Application Forms are available on the Intranet - search for ‘RIPA’.

Appendix A Flow chart of RIPA process



Appendix B Authorising Officers

Authorising officers are listed below. The Monitoring Officer will keep this list under review and will amend it in response to any staffing or service changes. Authorising officers should not be directly involved in the investigation.

1. Authorising officers for Directed Surveillance and CHIS are:

    a. Chief Executive (for **all** applications)

    b. Assistant Director of Environment **(subject to the special rule (see below),** for **all** applications)

    c. Managing Director, Director of Finance and Head of Assurance for oneSource **(subject to the special rule (see below**), for applications **relating to oneSource Services only)**

2. Special rule

    If directed surveillance is *likely* or *intended* to result in the acquisition of confidential or legally privileged information, **only the Chief Executive** or, (in his/her absence) the person acting as the Head of Paid Service can authorise it..

    If the acquisition of confidential or legally privileged information is *intended,* it should only be authorised if there are **exceptional and compelling circumstances** justifying it.

    If a **juvenile or vulnerable person** is to be used as a CHIS, **only the Chief Executive** or, (in his/her absence) the person acting as the Head of Paid Service can authorise it.

    If knowledge of **legally privileged or confidential information** is *likely* to be acquired if a CHIS is used, **only the Chief Executive** or, (in his/her absence) the person acting as the Head of Paid Service can authorise it.

    A CHIS should never be deployed for deliberately acquiring legally privileged information.

    Great care must be taken, and enhanced safeguards must be applied, to the handling, minimising access, storage, retention and destruction of confidential or legally privileged information in accordance with human rights and data protection legislation.

    Prior consultation, with the Monitoring Officer or the Deputy Monitoring Officer is required if the special rule applies.

    Confidential information includes medical records, confidential journalistic material and confidential discussions between Members of Parliament and their constituents.

    Legally privileged information includes confidential communications between a lawyer and his/her client for the purpose of obtaining and the giving of legal advice or communications for the purpose of actual or contemplated legal proceedings.

3. Designated officers authorised to represent the Council in a Magistrates' Court are:

    a. Chief Executive
    b. Director of Legal & Governance
    c. Assistant Director of Environment
    d. Trading Standards Manager, Public Protection
    e. Public Protection Manager
    f. Food Safety Divisional Manager, Public Protection
    g. Licensing and Health & Safety Divisional Manager, Public Protection
    h. Trading Standards Specialists
    i. Metrology Partnership Manager, Public Protection
    j. Enforcement Team Leader
    k. Projects & Compliance Manager

    Additionally any solicitor holding a Practicing Certificate working for the Council can appear on its behalf on an application to the Magistrates Court.

4. The Public Protection Manager is the RIPA Coordinating Officer.

5. Interim Officers on temporary or permanent employment and in positions with RIPA responsibilities **must** undertake RIPA training before executing RIPA approvals.

Appendix C Home Office guidance on the use of the internet as a surveillance tool

The following in an extract from the Home Office Code of Practice on Covert Surveillance (August 2018)

Online covert activity

3.10 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

Example 1: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 2: *A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

Example 3: *A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

3.16 In order to determine whether a directed surveillance 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:

- Whether the investigation or research is directed towards an individual or organisation;

- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);

- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;

- Whether the information obtained will be recorded and retained;

- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

- Whether 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.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

Example: *Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

Appendix C Home Office guidance on distinguishing between people who volunteer information and the use of informants

The following in an extract from the Home Office Code of Practice on Covert Human Intelligence Sources (August 2018)

Identifying when a human source becomes a CHIS

2.24 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

2.25 Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

Example: *Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague.*

2.26 However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible, therefore, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes.