

Corporate Policy & Procedures Document on the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA)

- Use of Directed Surveillance
- Use of Covert Human Intelligence Sources
- Accessing Communications Data

Contents

Introduction	3
Policy Statement	4
Senior Responsible Officer	4
Authorising Officers Responsibilities	5
General Information on RIPA	7
What RIPA Does and Does Not Do.....	9
Types of Surveillance	10
Conduct and Use of a Covert Human Intelligence Source (CHIS)	14
Use of the Internet, Social Media and Online Selling Platforms	15
Juvenile Sources and Vulnerable Individuals	18
Acquisition of Communications Data under IPA	20
Authorisation Procedures.....	21
Grounds for Authorisation	22
Serious Crime and Non RIPA Surveillance.....	22
Confidential Material	24
Duration	25
Working with Other Agencies	25
Record Management.....	26
Consequences of Non Compliance.....	27
Oversight by Members.....	27
Concluding Remarks	28
Appendix 1: RIPA and IPA roles.....	29
Appendix 2: Flow chart outlining process for Directed Surveillance and CHIS.....	30
Appendix 3: List of Useful Websites	32
Appendix 4: Guidance for Authorising Officers.....	33
Appendix 5: Guidance for Applicants.....	36

The Regulation of Investigatory Powers Act 2000 refers to 'Designated Officers'. For ease of understanding and application this document refers to 'Authorising Officers'.

Introduction

This document is based on the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office's Covert Surveillance Code of Practice, Covert Human Intelligence Sources (CHIS) Code of Practice and the Investigatory Powers Act Codes of Practice in relation to communications data. It takes into account the oversight provisions contained in the revised Covert Surveillance Code of Practice and Part 3 of the Investigatory Powers Act which came into force in June 2019 and replaced many elements of the Regulation of Investigatory Powers Act 2000.

The authoritative position on RIPA is the Act itself and any Officer who is unsure about any aspect of this document should contact the Head of Regulatory Services or the Head of Law, for advice and assistance.

This document has been approved by elected members and is available from the Head of Regulatory Services.

The Corporate Director for City Operations will maintain the Central Register of all authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorising Officer to ensure that relevant form is submitted, for inclusion on the register, within 1 week of its completion.

This document will be subject to an annual review by the Head of Regulatory Services and will be approved by elected members.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlap with the Council's Information Technology policies and guidance, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000, the Data Protection Act 2018 and its Code Of Practice and the General Data Protection Regulations. RIPA forms should only be used where **relevant** and they will only be **relevant** where the **criteria** listed are fully met.

Policy Statement

The Council takes its statutory responsibilities seriously and will at all times act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard the Head of Regulatory Services is duly authorised to keep this document up to date and amend, delete, add or substitute relevant provisions, as necessary. For administrative and operational effectiveness, the Head of Regulatory Services is authorised to add or substitute Authorising Officers with the agreement of the Senior Responsible Officer.

It is this Council's Policy that

- All covert surveillance exercises conducted by the Council should comply with the requirements of RIPA
- An Authorisation will only be valid if initialled by a gatekeeper and signed by an authorising officer.
- Authorising 'Access to Communications data' will be restricted to the Head of Regulatory Services and the Trading Standards Operations Manager. The National Anti Fraud Network is the Single Point of Contact for purposes of Access to Communications Data.

Senior Responsible Officer

The revised Code of Practice recommends that each public authority appoints a Senior Responsible Officer. This officer will be responsible for the integrity of the process in place within the public authority to authorise directed surveillance; compliance with the relevant Acts and Codes of Practice; engagement with the Commissioners and Inspectors when they conduct their inspections and where necessary overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.

The Senior Responsible Officer should be a member of the corporate management team and for the purposes of this policy the Corporate Director City Operations has been so delegated. It is the responsibility of the Senior Responsible Officer to ensure that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Investigatory Powers Commissioner's Office. Where an inspection report highlights concerns about the standards of authorising officers, it is the responsibility of the Senior Responsible Officer to ensure these concerns are addressed.

Authorising Officers Responsibilities

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 specify the seniority of officers who are able to authorise surveillance activity . These are Directors, Head of Service, Service Manager or equivalent.

It is essential that Senior Managers and Authorising Officers take personal responsibility for the effective and efficient operation of this document.

It is the responsibility of the Senior Responsible Officer in conjunction with the Head of Regulatory Services to ensure that sufficient numbers of Authorising Officers receive suitable training on RIPA and this document, and that they are competent.

It will be the responsibility of those Authorising Officers to ensure that relevant members of staff are also suitably trained as 'Applicants'.

An authorisation must not be approved until the Authorising Officer is satisfied that the activity proposed is necessary and proportionate.

However, it will be the responsibility of the gatekeeper to review any applications prior to submission to the Authorising Officer. They should ensure that the correct form has been used. These are the latest Home Office forms and are available on gov.uk and that the applicant has obtained a Unique Reference Number (URN) from the Corporate Director City Operations Corporate Leadership Assistant. The gatekeeper should also ensure that the form has been correctly completed and contains sufficient detail and information to enable the authorising officer to make an informed decision whether to authorise the application.

The gatekeeper should also scrutinise the form to ensure that it complies with the necessity and proportionality requirements before the authorising officer receives the form. A gatekeeper should be a person with sufficient knowledge and understanding of the enforcement activities of the relevant public body, who should vet the applications as outlined above. Once the gatekeeper is satisfied with the application they should initial the form and submit any comments on the application in writing to the Authorising Officer and provide necessary feedback to the applicant. In order that there is consistency with the quality of applications the Head of Regulatory Services and Trading Standards Operation Manager will act as gatekeepers for the Council. It should be noted that the Head of Regulatory Services will not act as gatekeeper and Authorising Officer on the same application.

- **Necessary** in this context includes consideration as to whether the information sought could be obtained by other less invasive means, and that those methods have been explored and been unsuccessful or could have compromised the investigation. The Authorising Officer must be satisfied that there is necessity to use covert surveillance in the proposed operation. To be satisfied there must be an identifiable offence to prevent or detect before an authorisation can be granted on the grounds falling within sec 28(3)(b) and 29(3)(b) of RIPA. The application should identify the **specific offence** being investigated (**including the Act and section**) and the **specific point(s) to prove** that the surveillance is intended to gather evidence about. The applicant must show that the operation is **capable of gathering that evidence** and that such **evidence is likely to prove** that part of the offence.
- Deciding whether the activity is **proportionate** includes balancing the right to privacy against the

seriousness of the offence being investigated. Consideration must be given as to whether the activity could be seen as excessive. An authorisation should demonstrate how the Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate to what it seeks to achieve. A potential model answer would make it clear that the 4 elements of proportionality had been fully considered.

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

Authorising Officers must pay particular attention to Health & Safety issues that may be raised by any proposed surveillance activity. Approval must not be given until such time as any health and safety issue has been addressed and/or the risks identified are minimised.

Authorising Officers must ensure that staff who report to them follow this document and do not undertake any form of surveillance, or access communications data, without first obtaining the relevant authorisation in compliance with this document.

Authorising Officers must ensure when sending copies of any forms to the Corporate Director City Operations for inclusion in the Central Register, that they are sent via email marked **Strictly Private & Confidential**.

General Information on RIPA

The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires the City Council, and organisations working on its behalf, to respect the private and family life of citizens, his home and his correspondence.

The European Convention did not make this an absolute right, but a qualified right. Therefore, in certain circumstances, the City Council may interfere in an individual's right as mentioned above, if that interference is:-

- a. **In accordance with the law;**
- b. **Necessary;** and
- c. **Proportionate.**

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a '**covert human intelligence source**' ('**CHIS**') – e.g. undercover agents. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

Directly employed Council staff and external agencies working for the City Council are covered by the Act for the time they are working for the City 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 an Authorising Officer after scrutiny by a gatekeeper.

The Protection of Freedoms Act 2012 introduced two significant changes to the use of RIPA

1) All local authority authorisations to use RIPA can only be given effect once an order approving the authorisation is given by a Justice of the Peace.

2) Applications for directed surveillance by local authorities must first meet the 'directed surveillance crime threshold'. Directed surveillance may only be authorised to prevent or detect criminal offences that;

- Are punishable by a maximum term of at least 6 months imprisonment, or,
- Are related to the sale of alcohol or tobacco to underage persons.

In cases of conflict between the Policy or Reference Guide and relevant statutes or the statutory Code of Practice, the statute or statutory Code shall prevail.

A list of officers who may authorise Directed Surveillance is kept by the Corporate Director City Operations and the current list is attached at **Appendix 1**. This list will be updated annually. The designated gatekeepers for the Council are the Principal Trading Standards Operations Manager and the Head of Regulatory Services.

If the correct procedures are not followed, evidence may be dis-allowed by the courts, a complaint of mal-administration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the City Council and will, undoubtedly, be the subject of adverse press and media interest.

A flowchart of the procedures to be followed appears at **Appendix 2**. A list of useful websites is available at **Appendix 3**.

What RIPA Does and Does Not Do

RIPA does:

- Requires prior authorisation of directed surveillance
- Prohibits the Council from carrying out intrusive surveillance
- Requires authorisation of the conduct and use of a CHIS
- Require safeguards for the conduct and use of a CHIS
- Requires proper authorisation to obtain communication data
- Prohibits the Council from accessing 'traffic data'

RIPA does not:

- Make unlawful conduct which is otherwise lawful
- Prejudice or dis-apply any existing powers available to the City Council 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 obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

If the Authorising Officer or any Applicant is in any doubt, they should ask the Head of Regulatory Services or the Head of Law before any directed surveillance, CHIS, or Access to Communications is authorised, renewed, cancelled or rejected.

Types of Surveillance

‘Surveillance’ includes

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

Surveillance can be overt or covert.

Overt Surveillance

Most surveillance activity will be done overtly, that is, 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 Neighbourhood Warden walking through the estate).

Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise 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 owner/proprietor to check that the conditions are being met.

The following are NOT normally Directed Surveillance:

- Activity that is observed as part of normal duties, e.g. by an officer in the course of day-to-day work.
- CCTV cameras (unless they have been directed at the request of investigators) – these are overt or incidental surveillance, and are regulated by the Data Protection Act.

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) RIPA) It is about the intention of the surveillance, not about whether they are actually aware of it; it is possible to be covert in Council uniform where, for example, the person is intended to mistake the reason for the officer being there.

RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

Directed Surveillance

Directed Surveillance is surveillance which: -

- Is covert; and
- Is not intrusive surveillance;
- Is not carried out in 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; 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).

Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. 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. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

Examples of Expectations of Privacy:

Two people are holding a conversation on the street and, even though they are talking together in public, they do not expect their conversation to be overheard and recorded by anyone. They have a 'reasonable expectation of privacy' about the contents of that conversation, even though they are talking in the street.

The contents of such a conversation should be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation and otherwise than by way of an immediate response to events.

A Surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation.

Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

For the avoidance of doubt, only those officers designated as 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this document, are followed.

Reconnaissance- Examples

Officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. If the officers chanced to see illegal activities taking place, these could be recorded and acted upon as 'an immediate response to events'. If, however, the officers intended to carry out the exercise at a specific time of day, when they expected to see unlawful activity, this would not be reconnaissance but directed surveillance, and an authorisation should be considered. Similarly, if the officers wished to conduct a similar exercise several times, for example to establish a pattern of occupancy of the premises

by any person, the accumulation of information is likely to result in the obtaining of private information about that person or persons and a directed surveillance authorisation should be considered.

Intrusive Surveillance

This is when it: -

- Is covert;
- Relates to residential premises and private vehicles; and
- Involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Only police and other law enforcement agencies can carry out this form of surveillance.

Council Officers must not carry out intrusive surveillance.

Notes about 'Intrusive'

Surveillance is generally 'Intrusive' only if the person is on the same premises or in the same vehicle as the subject(s) of the surveillance. Carrying out surveillance using private residential premises (with the consent of the occupier) as a 'Static Observation Point' does not make that surveillance 'Intrusive'. A device used to enhance your external view of property is almost never an *intrusive* device. A device would only become *intrusive* where it provided a high quality of information from inside the *private residential premises*. A device used to enhance your external view of property is almost never an *intrusive* device. A device would only become intrusive where it provided a high quality of information from inside the *private residential premises*. If premises under surveillance are known to be used for legally privileged communications, that surveillance must also be treated as *intrusive*.

Examples:

Officers intend to use an empty office to carry out surveillance on a person who lives opposite. As the office is on the 4th floor, they wish to use a long lens and binoculars so that they can correctly identify and then photograph their intended subject covertly. This is NOT intrusive surveillance, as the devices do not provide high quality evidence from inside the subject's premises. Officers intend using a surveillance van parked across the street from the subject's house. They could see and identify the subject without binoculars but have realised that, if they use a 500mm lens, as the subject has no net curtains or blinds, they should be able to see documents he is reading. This IS intrusive surveillance, as the evidence gathered is of a high quality, from inside the premises, and is as good as could be provided by an officer or a device being on the premises.

Examples of different types of Surveillance

Type of Surveillance	Examples
<u>Overt</u>	<ul style="list-style-type: none"> • Police Officer or Parks Warden on patrol • Sign-posted Town Centre CCTV cameras (in normal use) • Recording noise coming from outside the 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).
<u>Covert</u> but not requiring prior authorisation	<ul style="list-style-type: none"> • CCTV cameras providing general traffic, crime or public safety information.
<u>Directed</u> (must be RIPA authorised)	<ul style="list-style-type: none"> • 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. • Test purchases where the officer has a hidden camera or other recording device to record information that 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.
<u>Intrusive</u>	<ul style="list-style-type: none"> • Planting a listening or other device (bug) in a person's home or in their private vehicle. <p>THE COUNCIL CANNOT CARRY OUT THIS ACTIVITY AND FORBIDS ITS OFFICERS FROM CARRYING IT OUT</p>

Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

A Covert Human Intelligence Source (CHIS) is someone who establishes or maintains a personal or other relationship for the covert purpose or facilitating anything falling under the following bullet points;

- Covertly uses such a relationship to obtain information or to provide access to any information to another person or,
- Covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

RIPA may or may not apply in circumstances where members of the public volunteer information to the Council or to contact numbers set up to receive such information (such as benefit fraud hotlines). It will often depend on how the information was obtained. If an individual has obtained the information in the course of or as a result of a personal or other relationship it may be that they are acting as a CHIS. The contrast is between such a person and one who has merely observed the relevant activity from 'behind his (actual or figurative) net curtains.

A relationship is covert if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

If a person who volunteers information is then asked to obtain further information, it is likely that they would either become a CHIS or that a directed surveillance authorisation should be considered.

Examples of a CHIS may include:

- Licensing officers, working with the Police, covertly building a business relationship with a cab company which is believed to be using unlicensed drivers.
- Food safety officers posing as customers to get information on what is being sold at premises and developing a relationship with the shopkeeper beyond that of supplier and customer

What must be authorised?

Officers must not create or use a CHIS without prior authorisation. If there is any doubt as to whether an individual is acting as a CHIS advice should be sought from the Head of Regulatory Services.

- Creating (or "Conduct of") a CHIS means procuring a person to establish or maintain a relationship with a person so as to secretly obtain and pass on information. The relationship could be a personal or 'other' relationship (such as a business relationship) and obtaining the information may be either the only reason for the relationship or be incidental to it. Note that it can also include asking a person to continue a relationship which they set up of their own accord.

- Use of a CHIS includes actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

Use of the Internet, Social Media and Online Selling Platforms

The growth of the internet and the scale of information available online create significant opportunities for public authorities to gather material that can assist in preventing or detecting crime, carrying out statutory functions, and understanding or engaging with the public. Public authorities should make full and lawful use of such information. Much can be accessed without RIPA authorisation, and use of the internet prior to an investigation will not normally engage privacy considerations. However, if reviewing an individual's online presence becomes persistent, or if material is extracted, recorded, and retained such that privacy may be engaged, RIPA authorisations should be considered.

Use of the internet may itself constitute a covert surveillance technique where the subject is unaware monitoring is occurring. If conducted covertly for a specific investigation or operation and likely to yield private information, consider directed surveillance authorisation.

Where reasonable steps are taken to inform the public/individuals that monitoring may occur, activity may be overt and a directed surveillance authorisation will not normally be available. Information openly and commonly accessible (e.g., telephone directories, Companies House) generally carries a reduced expectation of privacy. Similarly, content posted to communicate with a wide audience may carry reduced expectations.

Where access controls/privacy settings are applied, the author generally has a reasonable expectation of privacy. Where such settings are available but not applied, data may be considered open source and authorisation is not usually required—but repeat viewings of “open source” content can, on a case-by-case basis, amount to directed surveillance.

Directed surveillance authorisation should be considered where online monitoring is systematic/persistent, directed at a person or group, and is likely to obtain private information, or where information is extracted and retained to build an intelligence picture (e.g., identity, habits, associations, pattern of life). If it is necessary and proportionate to covertly breach access controls, the minimum requirement is directed surveillance authorisation.

If someone acting for a public authority establishes or maintains a relationship online (i.e., goes beyond merely viewing/reading content) without disclosing their identity, a CHIS authorisation may be required. It is not unlawful to create a false identity, but doing so for a covert purpose without authorisation is inadvisable. Using photographs of other persons without permission to support a false identity may infringe other laws.

Preliminary, oneoff checks to see if a site or content is of interest—will usually not interfere with a reasonable expectation of privacy and will not normally require authorisation. Once activity becomes persistent or information is extracted/recorded/retained (particularly to build a profile), consider directed surveillance (and CHIS if relationships are formed/maintained).

Name/number search: A simple search (name, address, number) to locate an online presence is unlikely to need authorisation. If the profile is then monitored or information extracted for retention because it is relevant to an investigation, authorisation should be considered.

Initial profile check: A one-off visit to assess relevance is unlikely to need authorisation. If, during that visit, information is extracted and recorded to develop a profile (identity, pattern of life, habits, intentions, associations), it may be advisable to have authorisation even for that single visit (purpose, scope, and likely privacy impact are key).

General monitoring (no specific investigation): Broad scanning to identify trends, indicators, or themes does not require RIPA. If this leads to discovery of previously unknown subjects and a decision is made to monitor them as part of an investigation or operation, authorisation should be considered.

Factors when deciding whether directed surveillance authorisation is required include:

- whether the proposed online activity:
- Is directed towards an identifiable individual or organisation;
- Is likely to result in obtaining private information about a person or group;
- Involves visiting internet sites to build an intelligence picture or profile;
- Will result in information being recorded and retained;
- Is likely to reveal a pattern of life;
- Will be combined with other sources such that it amounts to information about a person's private life;
- Forms part of an ongoing piece of work involving repeated viewing;
- Is likely to capture third party information (friends/family/associates), creating collateral intrusion.
- Internet searches by a third party or use of a search/monitoring tool on behalf of a public authority may still require directed surveillance authorisation, depending on the purpose, persistence, and privacy impact. Using automated tools to detect generic terminology linked to illegal activity, or conducting general data analysis (e.g., predictive hotspotting, trend analysis) is not usually directed surveillance when not targeted at specific individuals as part of an investigation.
- Officers must adhere to the following prohibitions and constraints to prevent basic research from becoming surveillance:
 - No setting up of false profiles.
 - No bypassing of security/access controls.
 - No gathering of private information.
 - No repeated viewing of individuals' accounts, even if public/unprotected.

Any approved research should be recorded, including date, sites visited, and reason/necessity. Records must be available for inspection by the Investigatory Powers Commissioner's Office (IPCO). If research identifies a need to capture online evidence (e.g., screenshots of an

offence), this should be recorded and stored in line with local policy. These measures help eliminate the risk of basic online research slipping into covert surveillance without appropriate authorisation.

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 deployment. 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 on- going operation or investigation, authorisation should be considered.*

Juvenile Sources and Vulnerable Individuals

Section 4 of the Covert Human Intelligence Sources revised code of practice provides for special considerations for certain authorisations

Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On **no occasion can a child under 16 years of age be authorised to give information against his or her parents.**

Authorisations for juvenile CHIS must not be granted unless: -

- A risk assessment has been undertaken as part of the application, covering the physical dangers and the psychological aspects of the use of the child
- The risk assessment has been considered by the Authorising Officer and he is satisfied that any risks identified in it have been properly explained; and
- The Authorising Officer has given particular consideration as to whether the child is to be asked to get information from a relative, guardian or any other person who has for the time being taken responsibility for the welfare of the child.

Only the Chief Executive may authorise the use of Juvenile Sources. The Investigatory Powers Commissioner must be informed within seven working days of a CHIS authorisation of a juvenile source.

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 will only be authorised to act as a source in the most exceptional of circumstances.

Only the Chief Executive may authorise the use of Vulnerable Individuals. The Investigatory Powers Commissioner must be informed within seven working days of a CHIS authorisation of a vulnerable individual.

Test Purchases

Carrying out test purchases will not 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 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 also directed surveillance.

Please also see below under 'Serious Crime'

Anti-social behaviour activities (e.g. noise, violence, racial harassment etc)

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.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues.

Placing a covert stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

Acquisition of Communications Data under IPA

There are circumstances when “Communications Data” (CD) is permitted to be obtained from Communications Service Providers (CSPs). Part 3 of the Investigatory Powers Act 2016 (IPA) contains provisions relating to authorisations for obtaining communications data. This part of the Act came into force on 11 June 2019 and replaced many of the provisions in RIPA.

IPA governs how Local Authorities use the investigatory powers available to them. These powers provide for the lawful acquisition of Communications. Communications Data includes the ‘who’, ‘when’, ‘where’, and ‘how’ of a communication, but not the content i.e. what was said or written. Local Authorities may only acquire less intrusive types of Communications Data; “Entity data” (e.g. the identity of the person to whom services are provided) or “Events Data” (e.g. the date and time sent, duration, frequency of communications). Local Authorities are prohibited from obtaining the content of any communication.

The acquisition of Communications Data by a local authority is no longer subject to judicial approval by a magistrate. Applications for Communications Data are subject to independent examination, scrutiny and approval by the Investigatory Powers Commissioner’s Office. Local Authority Service (e.g. Trading Standards) applications for Communications Data are submitted to the IPCO through a service provided by the National Anti-Fraud Network (NAFN).

The Trading Standards Service collaborates with NAFN to maintain compliance with IPA and to ensure any application follows best practice. The Trading Standards Service consults and works with NAFN throughout the application process to ensure the legal basis for all applications are met. NAFN will act as a Single Point of Contact between both the CSPs and the Trading Standards Service concerning the request and provision of Communications Data. More practical guidance on the process and procedure for making Communications Data checks is available directly from Trading Standards.

Trading Standards will not acquire Communications Data unless an application for authorisation is approved by the Investigatory Powers Commissioner’s Office (IPCO). In respect of applications for Communications Data made under the IPA, the “applicable crime purpose” must be met concerning all applications for both Entity Data and Events Data. The applicable crime purpose is defined differently in relation to each of these data types. Where the Communications Data sought is Entity Data, the applicable crime purpose is the prevention or detection of crime or the prevention of disorder. Where the Communications Data is wholly or partly Events Data, the applicable crime purpose is defined as preventing or detecting serious crime (the serious crime threshold).

IPCO will only retain the Communications Data applications and decisions for a limited period of time, therefore the Trading Standards Service keep records of both the applications and the decisions received from the IPCO, as required.

Authorisation Procedures

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. **Appendix 2** provides a flow chart of the process to be followed.

Authorising Officers

Directed surveillance and or the use of CHIS can only be authorised by the officers listed in this document attached at Appendix 1. Authorising officers should ensure that they undertake at least one refresher training course on RIPA during each calendar year. The list will be kept up to date by the Corporate Director City Operations and amended as necessary. The SRO can add, delete or substitute posts to this list as required.

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management. RIPA authorisations are for specific investigations only and must be renewed or cancelled once the specific surveillance is complete or about to expire.

Only the Chief Executive can authorise the use of a CHIS who is a juvenile or a vulnerable person or in cases where it is likely that confidential information will be obtained through the use of surveillance.

Training Records

A certificate of attendance will be given to anyone undertaking training in relation to the use of RIPA. Training will be recorded on their individual learning and development plan.

Application Forms

Only the currently approved forms, available on the Home Office website, may be used. Any other forms will be rejected by the gatekeeper/authorising officer.

A gatekeeper role will be undertaken by either the Head of Regulatory Services or the Trading Standards Operations Manager who will check that the applications have been completed on the correct forms, have a URN and that they contain sufficient grounds for authorisation. They will provide feedback to the applicant and will initial the forms before being submitted to the authorising officer.

The Head of Regulatory Services can fulfil both the role as gatekeeper and authorising officer but will not fulfil both roles for an individual application.

Grounds for Authorisation

Directed Surveillance or the Conduct and Use of the CHIS can be authorised by an Authorising Officer where he believes that the authorisation is necessary in the circumstances of the particular case. For local authorities the only ground that authorisation can be granted is;

- For the prevention or detection of crime
- Or preventing disorder

Serious Crime and Non RIPA Surveillance

Serious Crime

From 1st November 2012, the Protection of Freedoms Act introduced an additional requirement for officers seeking to use directed surveillance or CHIS. From this date, with the exception of Trading Standards' work regarding test purchases for alcohol and tobacco, all applications must meet the 'serious crime' threshold. This has been identified as any offence for which the offender could be imprisoned for 6 months or more. An analysis of relevant offences indicates that covert surveillance may therefore be used by, Trading Standards (various offences including doorstep crime and counterfeiting), Waste Enforcement (fly tipping), Fraud against the Council and Child Protection and Adult Safeguarding issues. Where an offence meets the serious crime threshold, the applicant will apply to the Authorising Officer in the normal way via a gatekeeper, but will then need to attend Magistrate's Court to obtain judicial sign off.

Non RIPA Surveillance

This new process will automatically restrict the use of surveillance activity under the RIPA framework by a number of our services as the offences they deal with do not meet the serious crime threshold.

RIPA does not grant any powers to carry out surveillance, it simply provides a framework that allows authorities to authorise surveillance in a manner that ensures compliance with the European Convention on Human Rights. Equally, RIPA does not prohibit surveillance from being carried out or require that surveillance may only be carried out following a successful RIPA application.

Whilst it is the intention of this Authority to use RIPA in all circumstances where it is available, for a Local Authority, this is limited to preventing or detecting crime and from 1st November 2012 to serious crime. The Authority recognises that there are times when it will be necessary to carry out covert directed surveillance when RIPA is not available to use. Under such circumstances, a RIPA application must be completed and clearly endorsed in red 'NON-RIPA SURVEILLANCE' along the top of the first page. The application must be submitted to a RIPA Authorising Officer in the normal fashion, who must consider it for Necessity and Proportionality in the same fashion as they would a RIPA application. The normal procedure of timescales, reviews and cancellations must be followed. Copies of all authorisations or refusals, the outcome of reviews or renewal applications and eventual cancellation must be notified to the Corporate Director City Operations who will keep a separate record of Non-RIPA activities, and monitor their use in the same manner as RIPA authorised activities.

Assessing the Application Form

Before an Authorising Officer authorises an application, **they must**

Be mindful of this Corporate Policy & Procedures Document

Satisfy themselves that the RIPA authorisation is

- **in accordance with the law,**
- **Necessary** in the circumstances of the particular case on the ground specified above; and
- **Proportionate** to what it seeks to achieve

This means that they must consider

- whether other less invasive methods to obtain the information have been considered. The least intrusive method will normally be considered the most proportionate unless for example it is impractical or would undermine the investigation.
- balance the right of privacy against the seriousness of the offence under investigation. When considering necessity and proportionality, an authorising officer should spell out in terms of the 5 W's, (who, what, why, where, when and how) what specific activity is being sanctioned.
- Take account of the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**).
- Ensure that measures are taken wherever practicable to avoid or minimise collateral intrusion.
- Set a date for review of the authorisation and review on only that date where appropriate.
- Ensure that the form carries a unique reference number
- Ensure that the applicant has sent a copy to the Corporate Director City Operations for inclusion in the Central Register within 1 week of the authorisation.
- Ensure that the application is cancelled when required.

NB the application **MUST** make it clear how the proposed intrusion is necessary and how an absence of this evidence would prejudice the outcome of the investigation. If it does not then the application **SHOULD** be refused. Some guidance on how to complete the form for both authorising officers and applicants is available at **Appendix 4** and **Appendix 5**

Retention and Destruction of the Product

Where the product of surveillance could be relevant to pending or future legal proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period. This should be in line with any subsequent review. Attention should be drawn to the requirements of the Code of Practice issued under the Criminal Procedures and Investigations Act 1996. This states that material obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

There is nothing in RIPA 2000 which prevents material obtained from properly authorised surveillance being used in other investigations. However we must be mindful to handle store and destroy material obtained through the use of covert surveillance appropriately. It will be the responsibility of the Authorising Officer to ensure compliance with the appropriate data protection

requirements and to ensure that any material is not retained for any longer than is necessary. It will also be the responsibility of the Authorising Officer to ensure that the material is disposed of appropriately.

Confidential Material

Particular care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved.

Confidential Information consists of matters subject to legal privilege, confidential personal information or confidential journalistic information. So for example extra care should be taken where through the use of surveillance, it would be possible to obtain knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality, or legal privilege may be involved.

Where it is likely, through the use of surveillance, that confidential information will be obtained, authorisation can only be granted by Heads of Service or in their absence the Chief Executive.

Descriptions of what may constitute legally privileged information are set out in section 98 of Police Act 1997 and further guidance is set out in Paragraphs 9.1 – 9.6 of the Covert surveillance and property interference code of practice

Confidential Personal Information and Confidential Journalistic Information

Similar considerations to those involving legally privileged information must also be given to authorisations that involve the above. 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. This information can be either written or oral and might include consultations between a doctor and patient or information from a patient's medical records. Spiritual counselling means conversations between an individual and a Minister of Religion acting in an official capacity, where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

Confidential journalistic material includes material acquired or created for the purpose of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

Further information or guidance regarding Confidential Information can be obtained from the Head of Law.

Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, the Authorising Officer **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; At all times there will be a person designated to deal with the CHIS on behalf of the authority and for the source's security and welfare. This person should be in at least the position of Head of Service.
- 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; and
- Ensure **records** contain particulars and are not available except on a need to know basis

Records must be kept that contain the information set out in Statutory Instrument 2000/2725 – The Regulation of Investigatory Powers (Source Records) Regulations 2000. Further guidance on the requirements can be obtained from the Head of Regulatory Services.

Duration

The application form **must be reviewed in the time stated and cancelled** once it is no longer needed. The 'authorisation' to conduct the surveillance lasts for a maximum of 3 months for Directed Surveillance and 12 months for a Covert Human Intelligence Source.

Authorisations can be renewed in writing when the maximum period has expired. 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.

Urgent authorisations, if not ratified by written authorisation, will cease to have effect after 72 hours, beginning from the time when the authorisation was granted.

Working with Other Agencies

If an officer wishes to utilise the CCTV system operated by the Police

Directed Surveillance Authorisation must be obtained before an approach is made to the Control Room. If immediate action is required an Authorisation must be obtained within 72 hours of the request being made.

When some other agency has been instructed on behalf of the City 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.

When another Enforcement Agency (e.g. Police, HMRC etc):

- Wish to use the City Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures. Before any Officer agrees to allow the City Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form, or written confirmation that a Directed Surveillance Authorisation is in place.

- Wish to use the City Council's premises for their own RIPA action, the Officer should, normally, co-operate with the same, unless there is security or other good operational or managerial reasons as to why the City Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the City Council's co-operation in the agent's RIPA operation. In such cases, however, the City Council's own RIPA forms should not be used as the City Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

Record Management

A Central Register of all Authorisation Forms will be maintained and monitored by the Corporate Director City Operations

Records maintained in the Department

- 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 Authorising Officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation, together with supporting
- Documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the Authorising Officer;
- The Unique Reference Number for the authorisation (URN).

Central Register maintained by City Operations

Authorising Officers must forward details of each form to the Corporate Director City Operations Corporate Leadership Assistant for the Central Register, **within 1 week of the authorisation, review, renewal, cancellation or rejection.**

Records will be retained for six years from the ending of the authorisation. The Investigatory Powers Commissioner's Office (IPCO) and the Interception Commissioner can audit/review the City Council's policies and procedures, and individual authorisations.

Consequences of Non Compliance

Where covert surveillance work is being proposed, this Policy and Guidance must be strictly adhered to in order to protect both the Council and individual officers from the following:

- **Inadmissible Evidence and Loss of a Court Case / Employment Tribunal / Internal Disciplinary Hearing** – there is a risk that, if Covert Surveillance and Covert Human Intelligence Sources are not handled properly, the evidence obtained may be held to be inadmissible. Section 78 of the Police and Criminal Evidence Act 1984 allows for evidence that was gathered in a way that affects the fairness of the criminal proceedings to be excluded. The Common Law Rule of Admissibility means that the court may exclude evidence because its prejudicial effect on the person facing the evidence outweighs any probative value the evidence has (probative v prejudicial).
- **Legal Challenge** – as a potential breach of Article 8 of the European Convention on Human Rights, which establishes a “right to respect for private and family life, home and correspondence”, incorporated into English Law by the Human Rights Act (HRA) 1998. This could not only cause embarrassment to the Council but any person aggrieved by the way a local authority carries out Covert Surveillance, as defined by RIPA, can apply to a Tribunal – see section 15.
- **Offence of unlawful disclosure** – disclosing personal data as defined by the DPA that has been gathered as part of a surveillance operation is an offence under Section 55 of the Act. Disclosure can be made but only where the officer disclosing is satisfied that it is necessary for the prevention and detection of crime, or apprehension or prosecution of offenders. Disclosure of personal data must be made where any statutory power or court order requires disclosure.
- **Fine or Imprisonment** – Interception of communications without consent is a criminal offence punishable by fine or up to two years in prison.
- **Censure** – the Investigatory Powers Commissioner’s Office conduct regular audits on how local authorities implement RIPA. If it is found that a local authority is not implementing RIPA properly, then this could result in censure.

Oversight by Members

- Elected Members shall have oversight of the Authority’s policy and shall review that policy annually.
- The report to members shall be presented to the Elected Members by the SRO. The report must not contain any information that identifies specific persons or operations.
- Alongside this report, the SRO will report details of ‘Non-RIPA’ surveillance in precisely the same fashion
- Elected Members may not interfere in individual authorisations. Their function is to, with reference to the reports; satisfy themselves that the Authority’s policy is robust and that it is being followed by all officers involved in this area. Although it is elected members who are accountable to the public for council actions, it is essential that there should be no possibility of political interference in law enforcement operations.

Concluding Remarks

Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure may be that the action (and the evidence obtained), is held to be inadmissible by the Courts pursuant to Section 6 of the Human Rights Act 1998.

Obtaining an authorisation under RIPA and following this document will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

Authorising Officers should be suitably competent and must exercise their minds every time they are asked to sign the request. They must never sign or rubber stamp form(s) without thinking about their personal and the City Council's responsibilities.

Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

For further advice and assistance on RIPA, please contact the Head of Regulatory Services.

Directed Surveillance/CHIS Forms can be obtained from the Home Office website or from NAFN in relation to Access to Communications Data.

Appendix 1: RIPA and IPA roles

Roles for RIPA

Senior Responsible Officer - The Council's scheme of delegation appointed the Director of City Operations as the Senior Responsible Officer.

Authorising Officer – Head of Regulatory Services

Gatekeepers:

- Operation Manager - Trading Standards (or other service manager if use of surveillance powers are required)
- Head of Regulatory Services

Applicant – Officer in charge of investigation

Contact City Operations Corporate Leadership Assistant for a URN

Investigatory Powers Act 2016 (IPA) Roles

Legal Oversight - Director Governance & Law

Senior Responsible Officer - Director City Operations

Approved Rank Officers

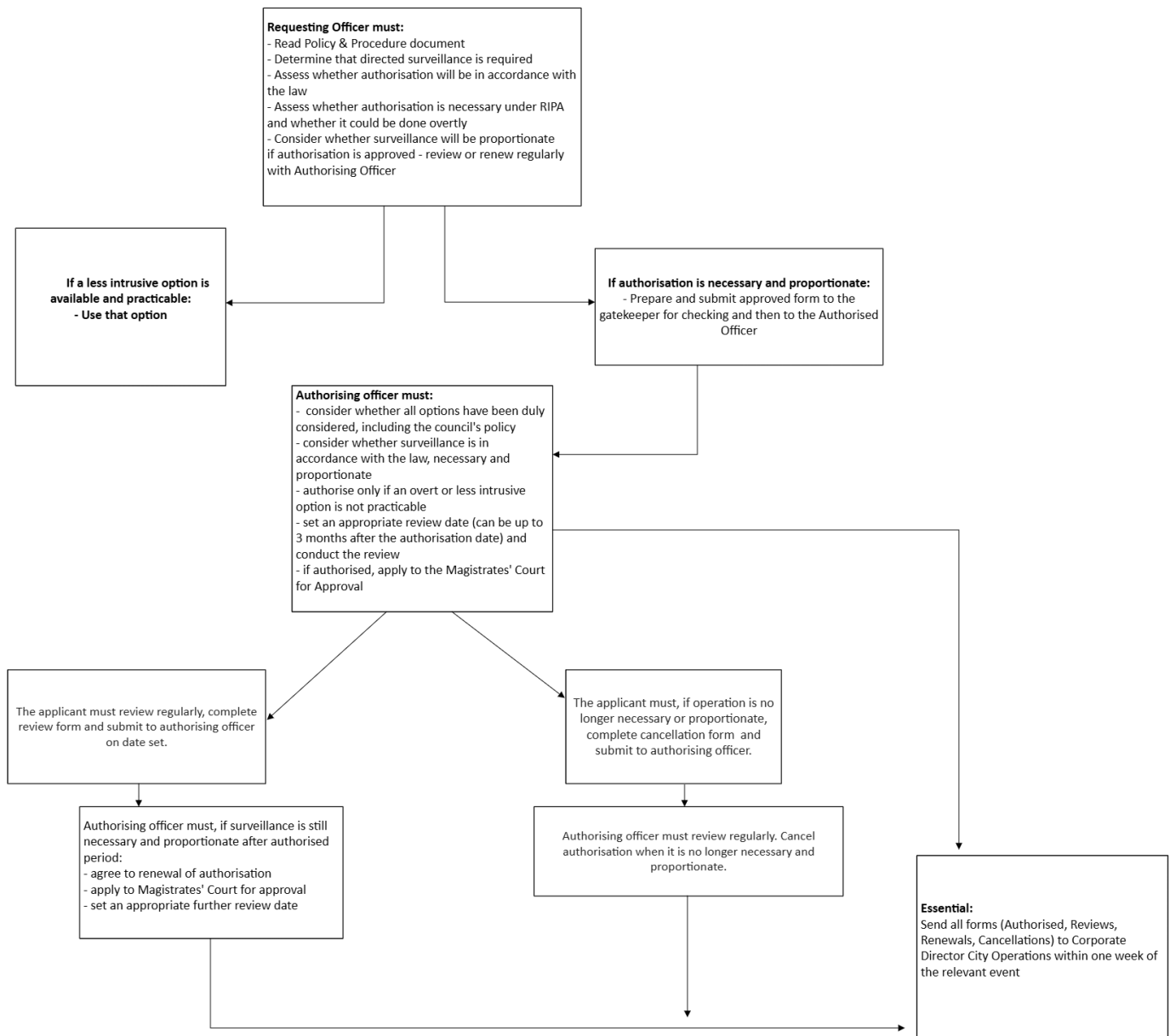
- Head of Regulatory Services
- Operations Manager - Trading Standards

Single Point of Contact for Accessing Communications Data

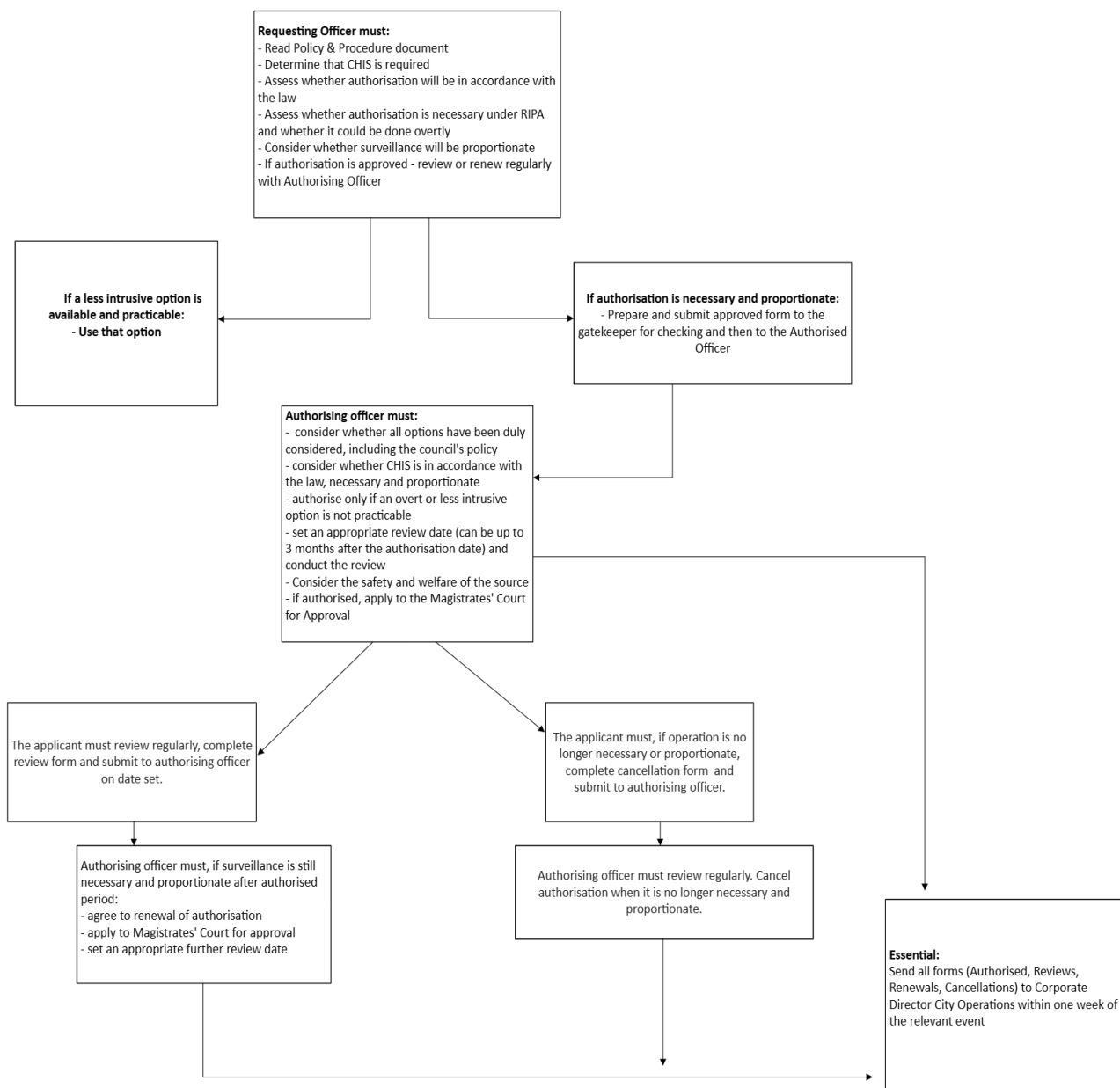
- National Anti Fraud Network (NAFN)

Appendix 2: Flow chart outlining process for Directed Surveillance and CHIS

Process for authorising Directed Surveillance



Process for authorising a CHIS



Appendix 3: List of Useful Websites

RIPA and IPA Forms, Codes of Practice and Advice

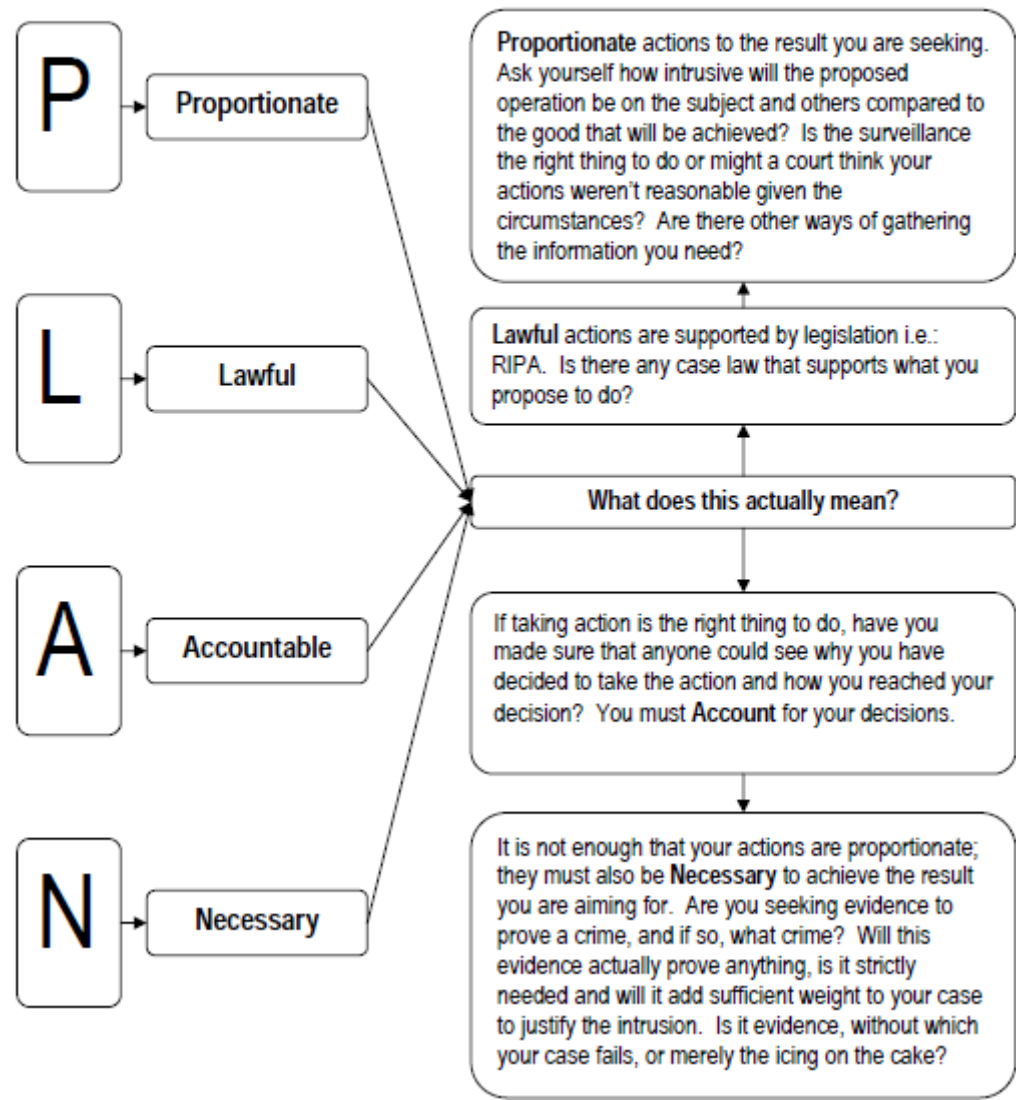
The policy requires you to use the most up-to-date versions of forms and codes of practice. Rather than reproduce forms and codes of practice that are subject to change, we have provided links to the currently approved versions. You should access the document you require by following the relevant link.

- The most up-to-date RIPA forms must always be used. These are available from the Home Office website and may be found by following this link :
www.gov.uk/government/collections/ripa-forms--2
- The full text of the RIPA Codes of Practice are available here :
www.gov.uk/government/collections/ripa-codes#current-codes-of-practice
- The full text of the IPA Codes of Practice are available here :
www.gov.uk/government/publications/communications-data-code-of-practice
- The Regulation of Investigatory Powers Act 2000 is available here:
<http://www.legislation.gov.uk/ukpga/2000/23/contents>
- The Investigatory Powers Act 2016 is available here:
[/www.legislation.gov.uk/ukpga/2016/25/contents](http://www.legislation.gov.uk/ukpga/2016/25/contents)
- The Investigatory Powers Commissioner's Office website has some useful information and advice and is available here :
www.ipco.org.uk

Appendix 4: Guidance for Authorising Officers

APPENDIX FOUR

Notes for Guidance for Authorisation – Directed Surveillance



Authorised Officer's Statement

12. Authorising Officer's Statement. (Spell out the "5 Ws" – Who; What; Where; When; Why and the following box.)

I hereby authorise directed surveillance defined as follows: (Why is the surveillance necessary directed against, Where and When will it take place, What surveillance activity/equipment is achieved?)

You must start by fully explaining what operation you are authorising. State why the surveillance is necessary to the case, what will be achieved, how it will be carried out, how many people used, what equipment / vehicles / technology you authorise the use of and where the operation will happen.

Make sure it is clear exactly what it is that you are authorising.

13. Explain why you believe the directed surveillance is necessary. [Code paragraph 2.4]

Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]

Now you must explain your decision. Simply stating that you "agree with the officer who applied for the reasons they gave" is not acceptable. You must give, in your own words, a detailed account of how you came to decide that the operation was necessary and proportionate. Make sure that you review the guidance in section seven and show how the evidence is necessary to the offence, and how the offence is one that it is necessary to investigate. Now ensure that you demonstrate how the officer has shown the need to obtain the evidence to be proportionate, when balanced against the person's expectation of privacy, the privacy of innocent third parties and the seriousness of the offence.

If you have completed a surveillance authorisation worksheet, go back over this as you should have already stated your reasons there.

You must explain why you feel it is in the public interest to carry out the action; is it serious, prevalent in the area, an abuse of position, premeditated? Why do you think that the investigation will be prejudiced without surveillance? Are you certain there is no other obvious and less intrusive way of obtaining the information? Does it need to be done? Record everything in this section.

This section must stand on its own, if you are called to court to justify your authorisation.

Authorised Officer's Statement

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with 3.1 to 3.12

This should be no more than four weeks from the date of authorisation. If you wish to restrict the length of time an officer may carry out surveillance for, you can use this box to set an early review date.

Date of first review

Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete dates after first review are known. If not or inappropriate to set additional review dates then leave

Use this box to record dates for review. The normal review period is no longer than every four weeks. It doesn't have to be completed but is useful to do so, especially when a shorter review period is appropriate.

This section is to be completed only by the Senior Authorised Officer if confidential information might be obtained. They should explain why they felt it to be appropriate for the surveillance to be carried out. To comply with the codes, show how further measures, such as more regular reviews and stricter limitations, have been put in place due to the particularly sensitive nature of the operation.

Name (Print)	Grade / Rank
Signature	Date and time
Expiry date and time [e.g.: authorisation on 30 June 2005, 23.59]	Expiry date and time [e.g.: authorisation on 1 April 2005 - expires]

Finally, write your name, sign the form giving the date and time. You must also record the expiry date. This is always three months, to the minute, from the date that the authorisation was given, no longer, or shorter. The operation can be cancelled before this date if appropriate. (See 7.14 (above) for guidance.)

Sections 15 and 16:

These sections relate to oral authorisations that may be granted or renewed only in urgent cases. In the case that an oral authorisation is granted, the AO should record the reasons why they considered the case urgent and why they believed it was not practicable to delay in order for the investigator to complete an application. Urgent oral authorisations last for seventy-two hours from the time of the authorisation. The officer carrying out the surveillance must complete a written application at the earliest opportunity, not necessarily at the end of the seventy-two hours.

Appendix 5: Guidance for Applicants

The RIPA 1 Form – Guidance Notes on Completion

Unique reference number. This must be provided by the Authorising Officer

Directed Surveillance Unique Reference Number (URN) (to be supplied by the central monitoring officer).

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Record your name. Not the name of the officers carrying out the surveillance (unless that is you).

What public body do you work for? Record it here

Public Authority (including full address)

What dept / unit do you work in? Record it here.

Unit/Branch/Division

Full address of your dept / office / building.

Full address

Contact details

You can give the operation a name if you wish.

Investigation/Operation Name (if applicable)

If the person who is the investigator in the case is someone other than you, record their name here.

Investigating Officer (if a person other than the applicant)

You must give the position of the Authorised Officer who will be reviewing the application. You do not need to give their name. This should be their full job title, rank or position.

Details of application:

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171. For local authorities exact position of the authorising officer should be given. For example, Head of Trading Standards.

Page Two

<p>What methods will you use for the surveillance? What are the technical aspects? Who, what, when, where, how long, how many, equipment etc. Mention everything. You will not be authorised to do things you don't mention here.</p>	<p>2. Describe the purpose of the specific operation or investigation.</p>	<p>Enter a summary of the reason for the operation and what you are planning to do. Be brief: what will you do, why are you doing it and what will you get out of it?</p>
	<p>3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.</p>	
	<p>4. The identities, where known, of those to be subject of the directed surveillance.</p> <p>Name:</p> <ul style="list-style-type: none"> Address: DOB: Other information as appropriate: 	<p>Who are you intending to gather evidence on? If you do not know the identity of all parties you must describe them as best as you are able.</p>
	<p>5. Explain the information that it is desired to obtain as a result of the directed surveillance.</p>	
	<p>What evidence do you intend to obtain from the surveillance? Specify exactly what you intend to get, how much and what types. This is so a judgement can be made on the weight of the evidence that you will get. Be careful what you write here: when you have achieved these aims the surveillance must stop immediately.</p>	

Page Three

<p>Specify the offences that you are investigating or preventing. State why the information has to be obtained by surveillance, why do you need it for the reason you specified? How is it essential to the case?</p>	<p>6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (SI 2003 No 3171)</p>	<p>Cross out the conditions that do not apply to you. In the case of a local authority, the only one that <i>does</i> is prevention or detecting crime or disorder.</p>
	<ul style="list-style-type: none">• In the interests of national security;• For the purpose of preventing or detecting crime or of preventing disorder;• In the interests of the economic well-being of the United Kingdom;• In the interests of public safety;• for the purpose of protecting public health;• for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;	
	<p>7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]</p>	
	<p>8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]</p>	
	<p>Describe precautions you will take to minimise collateral intrusion</p>	
	<p>Collateral intrusion is where the operation interferes with the private lives of those not intended to be subject to the surveillance. This could be members of the suspect's family, their partners, colleagues or members of the public. You must identify where there is a risk that you will gather this sort of information. You must take steps to minimise this risk and show that the risk left is unavoidable: what times are you conducting surveillance? Can you avoid catching others on camera? Do you have facilities to remove identifying features? The AO must be satisfied that the need to carry out the operation outweighs this risk.</p>	

Page Four

This is where you must justify your actions as proportionate. You should have completed a planner and decided that surveillance is necessary and the last resort. Record here what you have done already and what you cannot do as it'll prejudice the investigation. Tell the AO why the need to carry out the action outweighs the suspect's right to privacy. How serious is the matter? How intrusive will the operation be on the suspect and on others? What might happen if you don't carry out surveillance? Why can't you get the information in other ways? What will be achieved by gathering the evidence?

9. Explain why this directed surveillance is proportionate to what it is to be on the subject of surveillance or on others? And why is this surveillance in operational terms or can the evidence be obtained otherwise? (Code paragraph 2.5)

...ive might it
by the need for
s? (Code paragraph

10. Confidential information (Code paragraphs 3.1 to 3.12):

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's details

Name (print)		Tel No:	
Grade/Rank		Date	
Signature			

Confidential information is *special knowledge* of a person's religious, political or medical life or information of a confidential journalistic nature (journalistic sources). Communications subject to legal privilege are also confidential. If there is a chance that you might gather this sort of information, indicate the risk here. The authorisation can then only be given by the person within your public body designated by the RIPA code of practice for this purpose.

Finish by giving your name, telephone number, job title or rank. Date the form and sign it.

