Public Document Pack

Policy and Resources Committee

Date: THURSDAY, 21 JANUARY 2016
Time: 1.45 pm
Venue: COMMITTEE ROOMS, 2ND FLOOR, WEST WING, GUILDHALL

APPENDIX TO ITEM NO. 9

REGULATION OF INVESTIGATORY POWERS ACT 2000

John Barradell
Town Clerk and Chief Executive

This page is intentionally left blank

City of London

Regulation of Investigatory Powers Act 2000

Use of Covert Directed Surveillance

Use of Covert Human Intelligence Sources

Accessing Communications Data

Policy and Procedure

Adopted
27th June 2013

Revised
21st January 2016

1

INDEX

1. INTRODUCTION

The Regulation of Investigatory Powers Act 2000 ("the Act") came into force on 25 September 2000. The Act regulates the use of powers to *intercept communication data ("ICD")* and provides a framework for the authorisation and oversight of *directed surveillance ("DS")* and the use of *covert human intelligence sources ("CHIS")*. The Act was passed to ensure that law enforcement and other operations are consistent with the duties imposed on public authorities by the Human Rights Act (which incorporates the rights and freedoms of the European Convention on Human Rights into domestic law). It is unlawful for a public authority to act against a Convention right

This Policy and Procedure document sets out the means of compliance with, and use of, the Act by the City of London in its capacity as a local authority ("the Authority")[1] It is based upon the requirements of the Act and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources, together with the Revised Draft Code of Practice on Accessing Communications Data

The Authority has numerous statutory powers and duties to investigate the activities of private individuals, groups and organisations within its jurisdiction for the benefit and protection of the public (collectively known as the Authority's "Core Functions"). Such investigations may require the use of DS, CHIS and /or ICD. There are many reasons why the Authority might need to carry out investigations: e.g., audit investigations, benefit fraud, environmental health, Trading Standards, licensing and planning enforcement, control of building works. This list is not intended to be exhaustive. These areas are Core Functions and, as such, are covered by RIPA. Others, such as the investigation of its employees for the purpose of disciplinary procedures are not; and will, therefore, not fall within the RIPA framework.

For the purposes of this Policy and Procedure document, *surveillance* is deemed to include such ICD and, DS and the use of CHIS as the Authority is permitted to carry out under the Act. The Act provides for the authorisation of certain investigations using such surveillance.

The Authority's stated objective is compliance with the provisions of the Human Rights Act 1998 relating to the right to respect for privacy and family life, home and correspondence (in particular the provisions of Article 8 requiring respect for an individual's right to privacy). The right to privacy is a qualified right, not an absolute one. All investigations involve a breach of privacy to a greater or lesser extent and there are many circumstances where the Authority will have a legitimate reason to use ICD, DS or a CHIS as part of an investigation. The Act authorises such activities, so long as the investigation relates to a Core Function.

Before undertaking surveillance under RIPA, an authority must be satisfied that it is undertaken in connection with a Core Function. As all surveillance is likely to intrude upon someone's

[1] The City's powers as a *local authority* should be distinguished from its functions in its *private* capacity ie.i.e., as a freehold owner of landof land; under its City Cash functions (e.g. governing wholesale London markets such as Smithfield); and from its charity functions (e.g., under the Bridge House Estate and other charities). RIPA applies specifically to its local authority functions such as: enforcing trading standards, acting as a Port of Health authority, environmental protection and benefit fraud matters (see list at paragraph []) and "the Authority" should be understood in these terms.

human rights, it is important that the investigator is able to justify that the breach of privacy is: *necessary*, *proportionate* and *lawful*. It is also essential that the reasoning is fully documented and the correct authorisations gained (in order that the authority remains accountable for its actions).

The authoritative position on the Regulation of Investigatory Powers is, of course, the Act itself and any Officer who is unsure about any aspect of this Policy and Procedure document should contact, at the earliest possible opportunity, the Authority's *RIPA Monitoring Officer* for advice and assistance.

The Authority shall ensure that Officers with responsibility for authorising or carrying out surveillance or accessing communications data are aware of their obligations to comply with the Act and with this Policy. Furthermore, Officers shall receive appropriate training and/or be appropriately supervised in order to carry out functions under the Act. The List of Authorising Officers appears at Appendix One to this Document; however:

Even if a person is identified in the List, the person is not authorised to sign any RIPA forms unless they have been certified by the *RIPA Monitoring Officer* to do so.

NON-RIPA Activities

As a matter of law RIPA does not apply to investigations that do not form part of the Authority's Core Functions, but this does not preclude the Authority's investigators from using DS or CHIS in other circumstances. As an example, disciplinary investigations are NON-RIPA activities. The application of RIPA investigatory techniques would normally fail to meet the threshold of being *necessary*, *proportionate* and *lawful*. However, there may be circumstances where the threshold is reached, e.g., in cases of serious misconduct or criminal activity, particularly matters relating to City's Cash, and where covert monitoring may be used to gather evidence in a way which would not prejudice a criminal investigation or be prejudicial to the City's interests (see further the City's Code of Conduct and Communications & Information Systems Use policies).

It should be regarded as exceptional to engage in ICD, DS and the use of CHIS activities in relation to ordinary functions, such as disciplinary matters. In order to safeguard against abuse, it is the policy of this authority to apply RIPA principles to Non-RIPA investigations. This is to ensure proper adherence to human rights principles in all investigations. In the event that an investigation into a non-Core Function requires the use of these techniques, the investigator must apply in the same way, using the same forms, to the same Authorising Officer, endorsing the forms clearly in red ink, "NON-RIPA". Where disciplinary matters are concerned, the advice of Human Resources should also be sought.

It should be noted that such NON-RIPA activities would be undertaken at the Authority's own risk, as they are not afforded the legal protections noted in section 4 of this document.

In any case of doubt as to how NON-RIPA activities should be conducted, the Authority's *RIPA Monitoring Officer* should be contacted for advice and assistance.

The Authority appoints ~~**Lorraine Brook**~~**Neil Davies**, ~~Committee~~ Head of Corporate Performance and ~~Member Services~~Development ~~Manager~~, to discharge the functions of the *RIPA Monitoring Officer*/coordinator (RMO).

The Authority appoints **Susan Attard**, Deputy Town Clerk to discharge the functions of the "Senior Responsible Officer (SRO)."

This Policy shall be reviewed from time to time in light of changes in legislation, case law or for the better performance of the Policy. Authorising~~d~~ Officers must bring to the attention of the *RMO* any suggestions for continuous improvement of this Policy.

Failure to follow the provisions of this Policy (for example: carrying out surveillance without following the requirements of the Policy) is gross misconduct and will normally lead to disciplinary action.

A. Quick Checklist

Q: When is RIPA Authorisation required?
A: If the answer is **'Yes'** to all of the following questions:

A.1. Is the proposed activity 'surveillance'?

- involving monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording anything monitored, observed or listened to in the course of the proposed activity and/or a surveillance device will be used.

A.2. Is it 'covert'?

- carried out in a manner calculated to ensure that the target(s) will be unaware of the activity

A.3. Is it 'directed'?

- for the purposes of a specific investigation/operation.

A.4. Is it likely to result in obtaining private information about this person?

- information about the target /targets' private or family life is *likely* to be obtained.

A.5. Is it a 'foreseen/planned response'?

- something other than an immediate response to events. If the proposed activity has been planned in advance, it requires authorisation if all the answers to questions 1 to 4 above have also been 'Yes'.

A.6. Is it a 'core function' of the Authority?

- matters which relate to functions the Authority is required to carry out under statute (such as investigating benefit fraud or looking into allegations of fraudulent subletting).

If the answer is **'No'** to any of the above questions, the proposed activity falls outside the scope of RIPA and this policy

If the investigation relates to an 'ordinary function' of the Authority (i.e., disciplinary matters e.g. fake sickness or theft from the stationary cupboard, RIPA does not normally apply; however this Authority will treat NON-RIPA investigations in the same way as RIPA investigations and the rules below regarding applications will apply.

In any case of doubt, the advice of the *RMO* should be sought.

2. 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 course of authorised surveillance;
⇒surveillance by or with the assistance of appropriate surveillance devices

Surveillance can be intrusive, overt or covert.

Examples of different types of surveillance:

Type of Surveillance	**Examples**
Intrusive	Planting a listening or other device in a person's home or in their private vehicle.
THE AUTHORITY CANNOT AUTHORISE THIS ACTIVITY AND FORBIDS ITS OFFICERS FROM CARRYING OUT INTRUSIVE SURVEILLANCE.	
Overt	Car Park Patrol Officer on patrol Signposted CCTV cameras (in normal use) Recording noise from outside the premises, providing that the occupier has been warned that this will take place (e.g., where a statutory nuisance notice has been issued) Enforcement Officer conducting a site visit for monitoring purposes and determining whether a Notice or other formal legal action is appropriate providing any legislative requirements as to Notice have been complied with.
Covert Directed	Officers following an individual over a period to establish whether he is working whilst claiming benefit.

Intrusive Surveillance

RIPA does not authorise Local Authorities to carry out intrusive surveillance

Intrusive surveillance occurs when the surveillance is:

⇒ covert; and
⇒ 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 it was placed in the premises / vehicle.

The Authority's Officers must NOT carry out intrusive surveillance.

Notes about 'intrusive':

Surveillance is generally 'intrusive' only if the investigating officer is on the same premises or in the same vehicle as the subject(s) of the surveillance, or if it provides information about what is happening within a building. 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** *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 :

1. Officers investigating initial complaint about loud noise from a neighbour may use recording devices in the complainants flat to determine whether or not more formal legal action is appropriate (see 2.29 of the Code of Practice).

    - This is NOT intrusive surveillance.

2. *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*, so long as the devices do not provide high quality information from inside the subject's premises.

3. *Officers intend to use 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 information 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.*

Notes about 'Private Residential Premises' (PRP) :

Premises count as PRP if they are currently used as a residence, and this includes temporary use.

Examples :

- Flats, houses, caravans etc., used as a residence
- Hotel rooms
- Lorry cabs and camper vans
- A stairwell in a block of flats, known to be used by a homeless person as their temporary residence

The following are **NOT** PRP:

- Communal areas (like stairs in a block of flats)
- Canteens and dining areas
- Front gardens
- Setting up a local authority house for a covert operation (and, therefore) for non-residential purposes.

Overt Surveillance

Most of the surveillance carried out by the Authority will be done overtly. In many cases, Officers will be behaving in the same way as a member of the public, or will be going about Authority business openly (such as conducting a site visit for planning, licensing or nuisance enforcement purposes).

9

Similarly, surveillance will be overt if the subject has been notified that monitoring activity may be undertaken.

Covert Surveillance

For surveillance to be covert it must be carried out in a way that is intended to make sure that the subject of the surveillance is not aware that it is happening (Section 26(9)(a) RIPA). It is about the intention of the surveillance, not about whether they are actually aware of it. So, it is possible to be covert in Authority uniform where, for example, a person is intended to mistake the purpose of the officer's visit.

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

Directed Surveillance

Directed surveillance is surveillance which:

⇒ is covert; and
⇒ is not intrusive; and
⇒ is not carried out as an immediate response to events; and
⇒ 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 the purposes of the investigation).

The following are <u>NOT normally</u> Directed Surveillance:

- The covert recording or observation of suspected noise nuisance where the intention is only to record or witness excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels. In such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy and an authorisation may not be necessary.
- Activity that is observed as part of normal duties, e.g. by an officer in the course of day-to-day work recording noise levels from a commercial site.
- 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.
- Targeting a "*Hot spot*", e.g. licensing officers standing on a street to monitor illegal street trading or public nuisance where this is not part of a planned operation, or surveillance on fly tipping and dog fouling clear up (*refer to Home Office Guidance*).
- Routine visits to licensed premises to ensure compliance with their licence and/or the City Corporation's Statement of Licensing Policy and associated Code of Practice.
- ~~Test purchases for sale of alcohol to under 18s.~~

Private Information in relation to a person includes any information relating to his/her private and family life, his/her home and his/her 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 the person and (possibly others) that the person comes into contact, or associates, with.

Expectations of Privacy:

Examples:

1. ***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 required for a public authority to be able to record or listen to the conversation as part of a specific investigation or operation (although it would not be required where the investigation occurs as an immediate response to events).
2. **Where *surveillance of suspected noise nuisance from premises or the street takes place and where there is also a possibility of unintentional recording of conversations between persons in the street who are not being targeted, surveillance is not directed and authorisation will not be required for collateral intrusion alone. However steps must be taken in the planning and carrying out of the surveillance to minimise collateral intrusion.***
3. ***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.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases, overtly) obtained for the purposes of making a permanent record on that person, or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not.

Where such conduct includes surveillance, a directed surveillance authorisation may be required.

Reconnaissance

Reconnaissance does not normally require directed surveillance authorisation.

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 same 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 obtained.

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.

Use of Surveillance Information

There is nothing within RIPA that prevents evidence or intelligence gathered during the investigation of one matter, from being used for the purposes of a different investigation.

However, officers should exercise care in the secondary use of surveillance information, particularly where the evidence obtained is of a more sensitive nature.

Officers are reminded that it is their duty to ensure that the provisions of the Data Protection Act have been fully complied with in the further dissemination of surveillance information.

Officers are also reminded that it is their responsibility to ensure that dissemination protocols and safeguards are in place before further dissemination of surveillance information takes place.

3. CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

Who is a CHIS

A CHIS is someone who establishes or maintains a personal or other relationship for the covert purpose of using the relationship to obtain information. 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

RIPA does not normally apply in circumstances where members of the public volunteer information to the Authority or to contact numbers set up to receive such information (such as a benefit fraud hotline). If a member of the public volunteers information acquired in the course of, or as a result of the existence of, a personal or other relationship, then they are likely to be within the definition of a CHIS (RIPA section 26(8)c) If a person who provides information voluntarily is asked to obtain further information, they may either become a CHIS or DS authorisation should be obtained

Be careful not to create a CHIS by accident!

Examples:

- Licensing officers, working with the Police, covertly building a business relationship with a wholesaler believed to be supplying illegal street traders.
- Whistleblowing, when an employee is actively "recruited" to gather information on another employee the subject of a criminal investigation, provided this is undertaken within a formal framework (refer to the Authority's "Raising Concerns at Work (Whistleblowing)" Policy).
- Food safety officers posing as customers to get information on what is being sold from 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.

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, as well as the decision to use a CHIS in the first place.

Test Purchases

A normal test purchase does not usually involve the conduct or use of a CHIS. If the test purchase does not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information, the purchaser will not be a CHIS. In other words, if the purchaser acts in a manner entirely consistent with being an ordinary member of the public in making the test purchase, then no CHIS authorisation is needed.

However, if a relationship is developed with the person in the shop, for example, to obtain information about supplies of goods (for example, food unfit for human consumption), then this is likely to amount to the conduct or use of a CHIS. Similarly, if the test purchaser uses hidden devices, such as cameras or other recording devices, to record what is going on in the shop, then this will require authorisation, (albeit covert directed surveillance authorisation). In some instances, a combined authorisation may be required.

Note that it is not just members of the public who can be a CHIS; an officer acting as a test purchaser should be considered as a CHIS.

Use of juveniles as CHIS

A juvenile is a person under the age of 18. Special safeguards apply to the authorisation where the CHIS is a juvenile.

Authorisations for juvenile CHIS must not be granted unless:

⇒ A risk assessment has been undertaken as part of the application, covering the potential physical risks and the psychological aspects of the use of a child;

⇒ The risk assessment has been considered by the Authorising Officer who is satisfied that any risks identified have been properly examined; 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.

A person under the age of 18 must never be asked to give information against his parents or any person who has parental responsibility for him.

Authorisations must not be granted unless the Authorising Officer is satisfied that management arrangements exist which will ensure that an appropriate adult will be present at any meetings between Authority representatives and a CHIS who is under 18 years of age.

Authorisations for the use of a juvenile as a CHIS can only be granted by the Head of the Paid Service or, in his absence, the person acting as Head of the Paid Service.

Use of vulnerable individuals as a CHIS

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 unable to protect himself against significant harm or exploitation.

A vulnerable individual should only be authorised to act as a CHIS <u>in the most exceptional circumstances</u>.

Remember - authorisations for the use of a vulnerable individual as a CHIS can only be granted by the Head of the Paid Service or, in his absence, the person acting as Head of the Paid Service.

Additional notes on the conduct or use of CHIS can be found in the Home Office Code of Practice (see **Appendix Three)**.

4. AUTHORISATION PROCEDURES FOR DIRECTED SURVEILLANCE AND CHIS

Directed Surveillance and the conduct or use of a CHIS can only be lawfully carried out if properly authorised and if carried out in strict compliance with that authorisation. **Appendix Two** provides a flow chart of the process to be followed.

Authorising Officers

DS and CHIS can only be authorised by the Officers who are named in this Policy. The list of Authorising Officers appears at **Appendix One.** Authorising~~ed~~ Officers will be removed from the list if they do not attend the required training programmes or if they fail to meet the required nationally recognised standards. The Appendix will be kept up to date by the SRO and amended as needs require. In addition, the SRO has delegated authority to add, delete or substitute posts as required, in accordance with the section entitled 'Adoption and Amendments' below.

Authorisations under RIPA are separate from, and in addition to, any delegated authority that may be required under the Authority's Scheme of Delegation to Officers.

RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire.

Training Records

Authorising Officers must attend proper training before being entitled to authorise surveillance applications under this Policy. Training will be given or approved by the SRO who will maintain a central register of all those individuals who have undergone such training. Training must be undertaken every two years and must include an assessment of the delegate's competence.

Application Forms

Only the currently approved RIPA forms, available on the Home Office website, may be used. Any other forms will be rejected by the Authorising Officer and the RMO.

Grounds for Authorisation

Authorisation may be granted by an Authorising Officer where he believes that the authorisation is necessary in the circumstances of the particular case.

For **CHIS**, Section~~s 28(3) and~~ 29(3) of the ~~Act,~~Act set~~s~~ out the relevant grounds for establishing "necessity". These grounds are limited, in the case of local authorities, to being for:

"…the purpose of preventing and detecting crime or of preventing disorder".

For **Directed Surveillance**, an enhanced seriousness threshold came into force on 1st November 2012: [See Article 7A, Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Amendment Order 2003].

Seriousness Threshold *(This section came into force on 1st November 2012)*

It is important to note that, whilst covert surveillance may be thought of as useful touseful to a number of an authority's functions (such as nuisance information gathering, and regulating the workplace), RIPA Directed Surveillance is only available to local authorities when they are investigating criminal acts that (with some exceptions) carry a maximum sentence of at least 6 months imprisonment, or involve the sale of alcohol or tobacco to children:

Article 7A

"(1) An individual holding an office, rank or position with any county council or district council in England, a London borough council, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, or any county council or county borough council in Wales may not grant an authorisation under section 28 unless the conditions in paragraphs (2) and (3) are met.

(2) The first condition is that the authorisation under section 28 is for the purpose of preventing or detecting conduct which—

(a) constitutes one or more criminal offences, or

(b) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences.

(3) The second condition is that the criminal offence or one of the criminal offences referred to in the first condition is or would be—

(a) an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or

(b) an offence under—

(i) section 146 of the Licensing Act 2003(**a**) (sale of alcohol to children);
(ii) section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
(iii) section 147A of the Licensing Act 2003(**b**) (persistently selling alcohol to children);
(iv) section 7 of the Children and Young Persons Act 1933(**c**) (sale of tobacco, etc., to persons under eighteen)".

Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Amendment Order 2003

Authorising Officers may not use RIPA to authorise applications that do not meet the thresholds set out above.

Although RIPA is available to local authorities (and they are strongly advised to use RIPA to authorise directed surveillance and CHIS where appropriate) covert surveillance and the use of CHIS by a public body would not be unlawful merely because it was not authorised in accordance with RIPA.

The main advantage of following RIPA procedures is to:

- render the authorised activity lawful for all purposes;
- provide an audit trail to show that directed surveillance and the use of a CHIS has been carried out in a lawful manner;
- focus the mind on the Human Rights Act 1998;
- act as a reminder that the surveillance may have to be justified in other ways if the RIPA framework is not followed.

This Authority reminds all staff that covert operations may only be carried out if approved by an appropriate RIPA Authorising Officer.

Assessing the Application Form (the "Form")

Before an Authorising Officer signs a Form, they must:

- be mindful of this Policy and Procedures Document, the training provided and any other guidance issued, from time to time, by the RMO and SRO
- satisfy themselves that the RIPA authorisation ~~is :~~is:

  ⇒ **in accordance with the law ;**
  ⇒ **necessary** in the circumstances of the particular; and
  ⇒ **proportionate** to what it seeks to achieve.

Showing 'Necessity'

The application should identify:

- the specific offence being investigated (including section and statutory provision); and
- the specific allegations to be proved (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.

Showing Proportionality

In assessing whether the proposed surveillance method is proportionate:

- consider whether there are other methods of gathering the information. The least intrusive method will normally be considered to be the most proportionate method unless, for example, it is impractical or would undermine the investigation; and
- take into account the risk of intrusion to the privacy of persons other than the specified subject of the surveillance (**collateral intrusion**). Measures must be taken to avoid or minimise (so far as is possible) collateral intrusion and this may be relevant to the issue of proportionality.

Paragraph 74 of the Office of the Surveillance Commissioners' Procedures and Guidance sets out the essential elements of proportionality; "make clear that the following elements of proportionality (have) 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. providing evidence of other methods considered and why they were not implemented"

Completing the Application Form

On completing a Form, the Authorising Officer must:
~~; and~~

- set a date for the review of the authorisation and allocate a unique reference number for the application as follows:

Year / Division / Number of Application; and

- ensure that ~~a copy of~~ the RIPA form ~~is~~ and all supporting documents are forwarded to the RMO for entry onto the Central Register **within 48 hours of the relevant authorisation being given.**

The application MUST make it clear why the proposed intrusion is necessary and in what way the absence of the evidence to be gathered would have a prejudicial effect on the outcome of the investigation. If it does not, the application MUST be refused.

19

Additional Safeguards when authorising a CHIS

When authorising the use of a CHIS, the Authorisinged Officer **must also**:

- be satisfied that the **conduct** and/or the **use** of the CHIS is proportionate to what is sought to be achieved;
- be satisfied that **appropriate arrangements** exist for the management and oversight of the CHIS, this includes health and safety issues;
- consider the likely degree of intrusion on 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 to those persons who have a need to know.

~~**Urgent Authorisations**~~

~~Urgent Authorisations should not normally be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before the Authorising Officer is able to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. (A common example is where directed surveillance arises unexpectedly, during an officer's normal duties, and the officer needs to call the Authorising Officer for permission to continue).~~

~~If an officer wishes to obtain urgent oral authorisation for surveillance, the officer must telephone an Authorising Officer and provide the following information:~~

- ~~Full details of the person to be the subject of the surveillance;~~
- ~~The offence being investigated, and its seriousness;~~
- ~~How the investigation is necessary to the business of the Authority;~~
- ~~How the surveillance is necessary to the investigation;~~
- ~~Why the surveillance is proportionate, bearing in mind the offence, the expectation of privacy and the collateral intrusion; and~~
- ~~What the impact of ceasing surveillance and obtaining a written authorisation would be.~~

~~**Authorisation is not to be treated as urgent where the need for the authorisation is due to neglect or where the urgency is of the Authorising Officer's own making.**~~

~~**Urgent authorisations last for no more than 72 hours.** They must be recorded in writing on the standard form as soon as practicable and the extra boxes on the form must be completed to explain why the authorisation was urgent.~~

Duration

- The RIPA authorisation must be reviewed in accordance with its stated duration and cancelled once it is no longer needed.

- The authorisation to carry out /conduct the surveillance lasts for three months from authorisation, for directed surveillance, ~~and~~ twelve months from authorisation for an adult CHIS.

How to calculate the expiry of an authorisation:

An officer applies for permission to carry out surveillance, on a named subject, which is necessary to the proof of a case of serious fraud. The Authorising Officer considers that it is proportionate, and approves and signs the RIPA1 form at 3.35pm on 23rd March 2011.

Applications for *Directed Surveillance* last for three months.

The expiry is midnight on the final day of the authorisation: 22nd June 2011.

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

Authorisations can be renewed ~~when~~ before the maximum period has expired, and are subject to judicial approval. The Authorising Officer must consider the matter afresh, including taking into account the benefit 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.

~~In exceptional circumstances, renewals may be granted orally in urgent cases and these would last for a period of 72 hours.~~

To renew or not to renew?

Cases that are likely to be renewed would include the following:

- ~~Surveillance has shown that the case involves more people than originally suggested, and the surveillance operation is to be widened to gather evidence against those others.~~

- The surveillance has gathered three-quarters of the evidence required but is still crucially short of what is needed for a successful prosecution. The reason for this is that the investigator's car broke down on the last occasion.

Cases that are unlikely to be renewed would include the following:

- The investigators have been watching the subject for the last three months and have not seen him commit the offence. They are, however, sure he's 'at it' and would like another three months to have a look.

Confidential Information

The Act does not provide any special protection for "confidential information". Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information is involved.

Confidential information covers:
⇒ matters subject to legal privilege
⇒ communications between a Member of Parliament and another person on constituency matters
⇒ confidential personal information
⇒ confidential journalistic material.

Action which may lead to such confidential information being acquired is subject to additional safeguards under this Policy.

Material subject to legal privilege

Section 98 of the Police Act 1997 describes those matters that are subject to legal privilege. Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Thus legal communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. Privilege is not, however, lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

Legally privileged information is particularly sensitive and surveillance which acquires such material may engage Article 6 as well as Article 8 of the Human Rights Act 1998. Legally

privileged information obtained by surveillance is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover the fact that such surveillance has taken place may lead to related criminal proceedings being stayed as an abuse of process.

In locations where legal consultations are taking place, directed surveillance is treated for the purposes of RIPA, as intrusive surveillance. Local Authorities may not authorise *intrusive surveillance* using RIPA.

Confidential constituent information

Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

Confidential Personal Information

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of an individual (whether living or dead). Such information, which can include both oral and written communications, is held in confidence if held subject to an express or implied undertaking to hold it in confidence, or where it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

Spiritual counselling means conversations between an individual and a minister of religion acting in his 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 information

Confidential journalistic information includes material acquired or created for the purposes 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.

Additional Safeguards for Confidential Information

An application for the use of surveillance which is likely to result in the acquisition of confidential information should only be made in exceptional and compelling circumstances. Full regard should be had to the particular proportionality issues such surveillance raises.

The application for authorisation should, in addition to the reasons why it is considered necessary, contain:

⇒ an assessment of how likely it is that confidential information will be acquired;
⇒ indicate whether the purpose (or one of the purposes) of the use of surveillance or a CHIS is to obtain such confidential information.

Additional safeguards include: -

⇒ the Authorising Officer must the Chief Executive (as Head of the Paid Service) or, in his absence, the person acting as Head of the Paid Service;
⇒ those involved in the surveillance must be advised that confidential material may be obtained;
⇒ confidential material will not be retained or copied unless there is a clear, relevant and specific purpose for doing so;
⇒ confidential material will only be disclosed to those who have a clear and substantial need to know, and for a specific and proper purpose; confidential material must be clearly marked as such and accompanied by a clear warning as to its confidentiality.

If you have any doubt about the handling and dissemination of confidential information, seek advice from the Comptroller and City Solicitor *before* any dissemination of the material takes place.

Where an Authorising Officer authorises an application where confidential material may be obtained, it will be highlighted and drawn to the attention of the Surveillance Commissioner or his Inspector during the next available inspection.

Covert Surveillance Equipment

The use of recording devices in private residential premises, after the subject of the recording (normally a nuisance neighbour) has been told they will be monitored by the use of such devices, is not covert surveillance. It is overt surveillance as it constitutes monitoring. (Officers must, however, be aware of any risk to health and safety of the person permitting the use of their premises).

Set Up of Noise Monitoring or Recording Devices

Devices that make a record of noise levels are unlikely to be considered as a surveillance device requiring authorisation, provided the guidance in this section has been followed:

- Either the subject has been clearly informed that monitoring of sound levels using a noise recording device will be taking place, or
- devices that record sound are calibrated only to record noise likely to be audible at the recording location.

Devices that are not set up in accordance with the instructions in this section could be the source of complaints that they amount to unauthorised surveillance.

In the event that officers wish to do other than monitor noise by use of surveillance devices, they must seek urgent advice from the RMO. The rules under which covert surveillance equipment may be installed on private premises are complex, and RIPA may not authorise the Authority to install such equipment.

Surveillance equipment will only be installed in residential premises if a member of the public has requested help or referred a complaint to the Authority; or the appropriate authorisation to do so has been given. Any permission to locate surveillance equipment on residential premises must be agreed with the householder or tenant and documented in writing (i.e. a written log).

Surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle alone, do not necessarily constitute directed surveillance if no private information about any individual is obtained (as opposed to information about the location of that particular device). However, the subsequent use of that information coupled with other surveillance activity which may obtain private information, could interfere with Article 8 rights.

Examples where covert surveillance equipment might be used:

1. A contractor is suspected of stealing supplies. Officers gain authorisation to observe the supply depot and to photograph any persons entering or leaving and to video any loading or unloading that takes place, using a concealed video camera.

2. A benefit claimant is suspected of working in a market. Officers gain authorisation to observe the market stall and to photograph the subject, if he engages in trading activity, using a concealed still camera.

3. A person is suspected of mis-selling services to persons on the street. Officers gain authorisation to approach the man and record conversations with him, using a concealed recording device.

If it is likely to result in the obtaining of private information about an individual any request by an officer of the Authority to a resident to keep a video / audio as part of a covert evidence-gathering exercise will be regarded as a covert surveillance exercise conducted on behalf of the Authority and must be authorised appropriately. Requests for a written log concerning times, dates of disturbance and characteristics/location of source of problem evident to the complainant at the time of complaint would not be regarded as covert surveillance. **However, if a complainant is tasked to gather specific information, they should be considered a CHIS and therefore the appropriate authority must be sought.**

Access to the information gathered will generally only be allowed to limited and prescribed parties, including law enforcement agencies, and prosecution agencies, and will have special conditions attached to its use.

All information captured using a surveillance device and stored within recording media used during directed surveillance (or as part of the use of a CHIS) whether used or unused material, must be recorded and retained and revealed, in due course, to the prosecutor under the Criminal Procedure and Investigations Act (CPIA).

Additional notes on the conduct or use of CHIS, relating to the management of sources, taken from the Home Office's Code of Practice on CHIS can be found at Appendix Four**.**

Judicial Oversight *(This section came into force on 1st November 2012)*

The *Protection of Freedoms Act 2012,* brought into law the judicial oversight of all RIPA approvals by local authorities. It inserts sections into the 2000 Act which mean that authorisations and renewals made on or after 1st November 2012, whilst still given by local authority staff, do not take effect until a magistrate has approved them.

Judicial oversight does not take the place of the current authorisation process – it is an oversight function - not an authorisation function.

Once the application has been approved by an officer listed in Appendix One, the Authority must apply to the Magistrates' Court for an order confirming that:

- the person who granted or renewed the authorisation was entitled to do so;
- the grant or renewal met the relevant restrictions or conditions;
- there were reasonable grounds for believing (at the time it was made or renewed) that obtaining the information described in the form was both necessary and proportionate; and
- it is still (at the time the court considers the matter) reasonable to believe the grant/renewal to be both necessary and proportionate.

~~The application will often be dealt with without a formal hearing. It is possible for the matter to be determined at a hearing if the Court decides this, or the applicant makes a request for this to the Court.~~

CPR 2012 r.6 Section 2: General Rules

6.3 Exercise of court's powers

(1) Subject to paragraphs (2) and (3), the court may determine an application for an order, or to vary or discharge an order—

(a) at a hearing (which will be in private unless the court otherwise directs), or without a hearing; and

(b) in the absence of—

(i) the applicant,

(ii) the respondent (if any),

(iii) any other person affected by the order.

(2) The court must not determine such an application in the applicant's absence if—

(a) the applicant asks for a hearing…

The Judicial Review Form, (held on the Authority's intranet) must accompany all applications. The officer who made the initial application (normally the *Officer in Charge* of the case) must complete the form electronically, once the *Authorising Officer* has approved the application. (This also applies to requests for renewal of authorisations.)

Once the form has been completed, the applicant must submit this, along with electronic copies of any accompanying documents (set out in 7.15.7 below) to the *Authorising Officer* for checking. Once satisfied with the form and any attachments, the *Authorising Officer* must submit the bundle electronically to the ~~*RMO for*~~*RMO for* onward transmission to the court.

The bundle for submission to the court must include:

- the application for the order approving the authorisation;
- the authorised application or renewal form;
- any supporting information that, exceptionally, does not form part of the form;
- any information the applicant may have that might show a reason to refuse the application;
- an extract from the relevant legislation showing the offence being investigated and that it carries the relevant maximum sentence (unless it is one of the offences provided for in 7A(3)(b) of the 2010 regulations (see above); and
- a copy of **Appendix One** to this Policy, showing that the *Authorising Officer* is a person duly approved to carry out that function by the Authority.

The following should normally be disclosed to the Court when making the application:

Whether:-

- previous applications under RIPA have been made by the applicant and these have been turned down;
- there have been other investigations into the same subject or at the same address (regardless whether or not they were successful);
- the proposed subject or someone living with them has alleged harassment against any person associated with the Authority;
- there have been any complaints made to the Authority by the proposed subject or anyone living with them;

These are just examples – you must disclose anything that might influence a Magistrate in making their decision.

The form requires that the applicant makes a declaration of truth and disclosure, as part of the application for judicial approval. **It is important that this is not signed lightly;** check that all material facts have been disclosed within the bundle and that the contents are accurate and true.

6.3 Exercise of court's powers

(4) The court must not make, vary or discharge an order unless the applicant states, in writing or orally, that to the best of the applicant's knowledge and belief—

(a) the application discloses all the information that is material to what the court must decide; and

(b) the content of the application is true.

Once the bundle has been submitted, the *RMO* will note this in the Central Record. The applicant may not undertake the regulated activity until *judicial approval* has been given.

Within 24 hours of receiving notification of the Court's decision, the *RMO* will notify the *Authorising Officer* and the Applicant by sending them an email. The *RMO* will also send both parties copies of any court order and will retain the original in the *Central Record.* The *RMO* will note the record with the outcome.

If the Court decides to refuse the application, it will give two business days' notice allowing representations against the refusal to be made. The *RMO* will immediately notify the applicant and the *Authorising Officer* of this, and of the reasons for the proposed refusal. The applicant and the *Authorising Officer* will review the decision and notify the *RMO within* 24 hours if they wish to make representations to the Court before an order to refuse the application is made.

If the Authority decides to make representations about a refused application, the *Authorising Officer* must indicate whether a hearing should be held, or further written submissions made. The *RMO* will immediately notify the court officer of this and either request a hearing or indicate that a paper submission will be made.

If the submission is to be in writing, it must be drafted by the applicant and approved by the *Authorising Officer*. If must contain the standard declaration as set out above.

Challenging a Refusal

If the court refuses your request, it is required to give its reasons. Check the reasons carefully to see what they disclose:

You have omitted something from the application that makes it deficient in some way.	Rectify the deficiency and re-submit it to the court.
The magistrate has made a mistake of fact (for example: deciding that the offence you are investigating does not meet the seriousness criteria).	Evidence the correct facts and re- submit to the court.
The magistrate believes it is not proportionate *to investigate the matter in this way.*	Ensure that you have fully evidenced the impact of the matter on the community. Check that you have not sought to use disproportionate methods (such as seeking to carry out lengthy, mobile surveillance when short static surveillance would produce the required results).
The magistrate believes it is not necessary *to investigate the matter in this way.*	Ensure that you have clearly shown that the evidence you are seeking is essential to the case in hand. Check that you could not obtain the evidence by another means (such as open source investigations).
The Authorising Officer refers to other documents in reaching the decision to approve it but these documents are not attached to the submission.	Forward the missing documents to the court.

It is, obviously, far better that you carry out these checks <u>before</u> making the submission to the court.

If the Authority elects to seek a hearing, the applicant, *Authorising Officer* and *RMO will* attend the hearing[2].

At the conclusion of the hearing, the *RMO* will note the outcome in the Central Record.

[2] This Authority will normally seek a hearing of all such applications rather than applying for the application to be dealt with on paper. All hearings must be attended as indicated.

5. ACCESSING COMMUNICATIONS DATA

The Regulation of Investigatory Powers (Communications Data) Order 2003 gives the Authority power to acquire certain forms of communications data.

Communications Data

Communications data is defined in Section 21(4) of the Act. However, the Authority may only acquire communications data falling within sections 21(4) (b) and 21(4) (c) of the Act.

In essence, the Authority may acquire certain information held by communication service providers (CSPs) (telecom, internet and postal companies) relating to their customers.

Communications data does NOT include the content of any communication.

The Authority may only acquire communications data if it is necessary to do so for the purpose of preventing or detecting crime or of preventing disorder.

For the purposes of RIPA, detecting crime is defined as including:

- *establishing by whom, for what purpose and by what means and generally in what circumstances any crime was committed; and*

- *the apprehension of the person by whom any crime was committed*

Accessing Communications Data

The Act provides two different ways of authorising access to communications data: through an authorisation under section 22(3), or by a notice under section 22(4). An authorisation allows the Authority to collect or retrieve the data itself. A notice is given to a postal or telecommunications operator and requires the operator to collect or retrieve the data and provide it to the Authority. A Designated Person decides whether or not an authorisation should be granted or a notice given.

NB: For practical reasons, generally the Authority will only be using the notice route via NAFN to access communications data.

The applicant is a person involved in conducting an investigation or operation who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the Designated Person, the necessity and proportionality of a specific requirement for acquiring communications data.

Applications may be made orally in exceptional circumstances, but a record of that application must be made in writing or electronically as soon as possible.

Applications, which must be retained by the Authority, must:

⇒ include the name and position held by the person making the application;
⇒ include a unique reference number;
⇒ include the operation name (if applicable) to which the application relates;
⇒ specify the purpose for which the data is required, by reference to a statutory purpose under section 22(2) of the Act; (for local authorities this can only be for the purposes of section 22(2)(b) – prevention or detection of crime or of preventing disorder);
⇒ describe the communications data required specifying where relevant, any historic or future date(s) and, where appropriate, time period(s);
⇒ explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
⇒ consider and, where appropriate, describe any meaningful collateral intrusion; the extent to which the privacy of any individual not under investigation may be infringed; and why that intrusion is justified in the circumstances, and identify and explain the time scale within which the data is required.

Designated Person

The Designated Person is a person holding a prescribed office in the same public authority as the applicant, who considers the application and records his considerations at the time (or as soon as is reasonably practicable) in writing or electronically. If the Designated Person believes it appropriate, necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given.

Designated persons must ensure that they grant authorisations or give notices only for purposes and only in respect of types of communications data that a Designated Person of their office, rank or position in the relevant public authority may grant or give.

The Designated Person shall assess the necessity for any conduct to acquire or obtain communications data taking account of any advice provided by the Single Point of Contact (SPoC) (see below).

Designated persons should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, (although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons).

Individuals who undertake the role of a Designated Person must have current working knowledge of human rights principles, specifically those of *necessity* and *proportionality*, and how they apply to the acquisition of communications data under the Act.

Single Point of Contact (SPoC)

At the City of London Corporation, the SPoC for communications data will be accessed via the National Anti-Fraud Network (NAFN).

The SPoC is either an accredited individual or a group of accredited individuals trained to facilitate the lawful acquisition of communications data and effective co-operation between a public authority and CSPs. To become accredited, an individual must complete a course of training appropriate for a SPoC.

An accredited SPoC promotes efficiency and good practice by ensuring only practical and lawful requirements for communications data are undertaken. The SPoC applies objective judgement and advice to both the applicant and the Designated Person. In this way the SPoC provides a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner.

The SPoC should be in a position to:

⇒ assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
⇒ advise applicants and designated persons on interpretation of the Act, particularly whether an authorisation or notice is appropriate;
⇒ provide assurance to designated persons that authorisations and notices are lawful under the Act and free from errors
⇒ assess any cost and resource implications of data requirements to both the Authority and the CSP.

Public authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of communications data.

The SPoC may also be a Designated Person.

6. AUTHORISATION PROCEDURES FOR ACCESSING COMMUNICATIONS DATA

Accessing communications data can only be lawfully carried out if properly authorised and if carried out in strict accordance with that authorisation. Generally, the Authority will only be using the notice route to access communications data, and will generally use the services provided by the National Anti-Fraud Network (NAFN) to do so.

Accessing Communications Data through NAFN

The Authority subscribes to the services provided by NAFN (nafn.gov.uk). Such services include intelligence gathering, support for investigative and enforcement activity undertaken authority-wide. NAFN employ experienced and qualified SPoC's, and provide a service for obtaining communications data under the Act.

The Authority's officers, operating in investigation and enforcement roles, are expected to be registered with NAFN, and are free to utilise the RIPA communication data services provided. The Authority's Designated Persons are likewise expected to be registered with NAFN for the purpose of reviewing and authorising RIPA communications data requests.

The Designated Persons registered with NAFN are listed at **Appendix One**.

NAFN SPoC's will consider and review each request made for communications data, assessing the legality, justification and proportionality of each request. NAFN will also work with the applicant to ensure that best practice is followed when making requests for communications data. Once approved by the Designated Person, NAFN will provide a court bundle for any judicial oversight, and obtain the required information from the communication provider(s) upon receipt of the court approval documentation.

Detailed guidance concerning the use of NAFN's RIPA Communications Data service is available to all registered users at www.nafn.gov.uk. Officers of the Authority are expected to familiarise themselves with this guidance, and follow both that guidance, and this Policy when making applications to access communications data.

The Authority will expect all requests for communications data under RIPA be made via NAFN, unless there is good reason for not doing so, in which case officers will be required to follow the guidance contained within this Policy below, and explain, in detail, their reasons for not requesting data through NAFN.

Designated Persons

Approval for the accessing of communications data can only be given by a 'designated person' who holds a certificate from the *RMO*. This is not to be confused with those officers authorising covert directed surveillance. A list of Designated Persons within the Authority for the purpose of approving access to communications data is contained within **Appendix One**. The Appendix will

be kept up to date by the RMO and amended as needs require. In addition, the RMO has the delegated authority to add, delete or substitute posts from the list as required.

Authorisations under RIPA are separate from, and in addition to, any delegated authority that may be required to act under the Authority's Scheme of Delegation to Officers.

RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete, or about to expire.

Training Records

Designated Persons must attend proper training before being entitled to sign any RIPA forms under this Policy. Training will be given or approved by the SRO who will maintain a Central Register of all those individuals who have undergone such training.

Application Forms

Only the currently approved RIPA forms, available on the Home Office website, may be used. Any other forms will be rejected by the SPoC.

Grounds for Application

An application for accessing communications data may be granted by a Designated Person where they believe that the authorisation is necessary in the circumstances of the particular case. However, the only statutory purpose under which the Authority can access communications data is for the prevention or detection of crime or the prevention of disorder.

Nature of Communications Data to be accessed

Only data falling within sections 21(4) (b) and 21(4) (c) of the Act may be accessed. This could be: the name of customer; address for billing; contact number; subscriber's account information, such as bill paying arrangements (but note the risk of collateral intrusion); services the customer subscribes to; activity including itemised records of telephone calls (numbers dialled;, internet connections; dates and times/duration of calls; text messages sent. In respect of postal items, data means anything written on the outside of the item.

Local Authorities are not permitted to use this procedure to access *traffic data* (as defined by section 21(4) (a) of the Act).

Assessing the Application Form

Once an applicant has completed the application form, it should be submitted to the SPoC for consideration.

The SPoC will either reject the application and provide the applicant with a Rejection Report setting out the reasons for the rejection, or prepare a SPoC Report and draft the notice which will be submitted to the Designated Person together with the application.

The Designated Person will consider the documentation received from the SPoC and before signing the application (and therefore approving the issue of a notice) must:

(a) be mindful of the Authority's Policy and Procedures Document, the training provided and any other guidance issued, from time to time, by the *RMO*;

(b) be satisfied that the RIPA authorisation is:
⇒ **in accordance with law;**
⇒ **necessary** in the circumstances of the particular case on the grounds available to the Authority, and
⇒ **proportionate** to what it seeks to achieve, and

In assessing proportionality, consider whether there are other methods of gathering the information. The least intrusive method will be the most proportionate method.

Communications Data Notice

The Designated Person should complete the Designated Person's Consideration Form and if appropriate sign the notice and return all documentation to the SPoC.

Single Point of Contact (SPoC)

The Authority has designated a SPoC, as detailed in **Appendix One**. The CSPs will only deal with notice requests from authorised/accredited SPoCs.

The SPoC has undergone accredited training and can:
⇒ assess whether access to the communications data sought is reasonably practicable for the postal or telecommunications operator;
⇒ advise applicants and Designated Persons on the practicalities of accessing different types of communications data from different postal or telecommunications operators;
⇒ advise applicants and Designated Persons whether the communications data sought falls into the categories of data which the Authority can seek;
⇒ provide safeguards for authentication;
⇒ assess any cost and resource implications to both the Authority and the postal or telecommunications operator.

Once in receipt of a duly issued notice from a Designated Person the SPoC will forward the notice to the CSP for action, and will act as the liaison between the Authority and the CSP.

Urgent Approvals

There is <u>no</u> provision for the Authority to grant urgent approvals for accessing communications data. Applications can only be made in the manner set out above.

Duration

The RIPA authorisation to access communications data lasts for a maximum of 1 month commencing when the authorisation is granted or the notice is given. An Authorising Officer can specify a shorter period, if that is satisfies the request, since this may go to the proportionality requirements.

For "future" communications data, disclosure may only be required of data obtained by the postal or telecommunications operator **within** this period.

For "historical" communications data, disclosure may only be required of data in the possession of the postal or telecommunications operator.

A notice may be renewed at any time during the month it is valid, by following the same procedure as for obtaining a fresh authorisation or notice. A renewed authorisation takes effect at the point at which the authorisation or notice it is renewing, expires.

An Authorising Officer shall cancel an authorisation or notice as soon as it is no longer *necessary*, or the conduct is no longer *proportionate* to what is sought to be achieved. **The duty to cancel a notice falls on the Authorising Officer who issued it**. In the case of a notice being cancelled, the relevant postal or telecommunications operator must be informed of the cancellation by the SPoC.

7. WORKING WITH / THROUGH OTHER AGENCIES

Where another agency (for example, Police, Department for Work and Pensions, HM Revenue and Customs etc.,) is jointly undertaking with the Authority any action under RIPA, the parties will agree which agency will make any necessary applications under RIPA and each party will be kept informed and will receive copies of any relevant documents (e.g. any RIPA application forms), as required. Where the Authority is requested to take the lead in any such investigation, this document and the forms in it must be used as normal, and the agency must be advised or kept informed, as necessary, of the various requirements of this Policy. They must be made explicitly aware of what they are authorised to do and provided with a copy of the authorised application form (which may, if necessary, be redacted).

Where the agency acts as a direct agent of the Authority (e.g. a private detective agency), this Policy and Procedure document, the relevant Forms and authorisation processes, must be followed. The use of an outside agent must be authorised by the RMO. The agent must be RIPA-compliant (i.e. have a full understanding of RIPA procedures) and must collect any evidence in accordance with RIPA and this Policy. All relevant applications to gather, use or produce evidence by the external agency must be made by the Officer in Charge and approved in accordance with this Policy. If judicial approval is required, the agent must give evidence and appear at court on the application on behalf of the Authority.

Where another agency wishes to use the Authority's resources (for example, a CCTV surveillance system or audio recording system), that agency must use its own RIPA procedures. Before any Officer agrees to permit the use of Authority resources, a copy of that agency's RIPA form must be obtained for the record, a copy of which must be passed to the *RIPA Monitoring Officer* in the usual manner, and / or relevant extracts from the form which are sufficient for the purposes of protecting the Authority and the use of its resources.

If, exceptionally, the outside agency claims that releasing a copy of the authorisation is not possible, the agency must provide a certificate from its authorising officer which clearly sets out the objectives, the authorised behaviour and the relevant dates, and which confirms that authority has been granted in accordance with RIPA.

If in doubt, consult with the *RMO* at the earliest opportunity.

8. THE "POLICING" OF RIPA

RIPA is overseen by Surveillance Commissioners, who are tasked to ensure that RIPA is being applied properly. Inspections are carried out at regular intervals. Information about inspections and the Office of the Surveillance Commissioner (OSC) can be found at www.surveillancecommissioners.gov.uk .

This Authority has, in following the general advice from the OSC, appointed an SRO who is responsible for corporate oversight of the RIPA process. The SRO is **Susan Attard**, who is the Authority's Deputy Town Clerk.

Any person who, being an employee of the local authority or person contracted to carry out duties by the local authority, knowingly or recklessly acts, or fails to act, in a way that tends to, or is likely to, obstruct or mislead any person carrying out the duties of an inspector during an inspection by the OSC, may have committed 'gross misconduct' and be liable to disciplinary proceedings.

Any person aggrieved by the way a local authority carries out covert surveillance as defined by RIPA can apply to a Tribunal under the Act for redress within a year of the Act complained of or any longer period that the Tribunal thinks it just and equitable to allow:

- the Tribunal can quash any authorisation and can order the destruction of information held or obtained in pursuit of it;

- it cannot, as yet, award compensation, but its findings may be of use in a human rights challenge or as a defence to a case brought by the Authority, or in a referral to the local government Ombudsman, or a complaint to the Information Commissioner, from which compensation awards can flow.

9. CONSEQUENCES OF NON-COMPLIANCE

Where covert surveillance is being proposed, this Policy and Guidance must be strictly adhered to in order to protect both the Authority 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 (both defined above) 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 rules on admissibility means that the court may exclude evidence because the 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 Authority but any person aggrieved by the way a local authority carries out covert surveillance, can apply to a Tribunal (section 15).

Offence of unlawful disclosure – disclosing personal data gathered as part of a surveillance operation, is an offence under Section 55 of the Act. Disclosure can only be made where the officer disclosing the information 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 Office of Surveillance Commissioners 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.

Disciplinary Action – Failure of officers to comply with this Policy or the relevant codes of conduct, is a disciplinary offence under the Authority's Human Resources Policies and Procedures.

10. COMPLAINTS

If any person complains about breach of this Policy, they will be directed to the Authority's Complaints Procedure, and invited to use it. ANY complaint received will be treated as serious and investigated in line with this Authority's policy on complaints.

The details of any operation, or indeed its existence, must not be admitted to as part of the complaint handling process. This ensures that any operational information will remain entirely confidential and will not be disclosed to the complainant.

Unlawful access or disclosure of information may be a contravention of the Data Protection Act 1998, and may be reported to the Data Protection Commissioner.

The Surveillance Tribunal is available to anyone who believes that their Article 8 rights have been unlawfully breached by an authority using the RIPA authorisation process. The 2000 Act establishes an independent Tribunal. The Tribunal has full powers to investigate and decide any case within its jurisdiction. Details of the Tribunal's procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

020 7035 3711.

Judicial Review remains available to any person who believes their rights have been unlawfully breached by reason of the use of investigatory powers covered by RIPA.

11. NON-RIPA SURVEILLANCE

RIPA does not grant powers to carry out surveillance - it simply provides a framework that allows Authorities to authorise and supervise 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 under RIPA**.

Whilst it is the intention of this Authority to use RIPA in all circumstances where it is appropriate (i.e. preventing or detecting crime or disorder), the Authority recognises that there are times when it will be necessary to carry out covert directed surveillance other than by using RIPA.

.

Non-RIPA Surveillance

If an investigation concerns internal matters that may lead to criminal proceedings, RIPA procedures may be appropriate.

Examples:

- the investigation of internal fraud allegations that a member of staff is claiming vehicle mileage allowances when they are actually using public transport. Where the evidence gathered against them is for disciplinary purposes only, RIPA does not apply as this is not a Core Function of the Authority;
- RIPA also would not cover civil proceedings to recover fraudulent expenses claims.

If, however the member of staff is to be prosecuted for fraud, RIPA may well be appropriate and in this Authority, RIPA procedures may well be used in such circumstances order to safeguard against abuses of a person's human rights

Under such circumstances, a RIPA application must be completed in accordance with this Policy and in accordance with the advice of Human Resources, and the application must be 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 under the **necessity** and **proportionality** tests in the same fashion as they would a RIPA application.

The normal procedure of timescales, reviews and cancellations must also be followed.

The authorisation or refusal of the request, the outcome of any reviews, renewal applications and eventual cancellation of the authorisation must be notified to the RMO in the normal way.

The RMO will keep a separate record of Non-RIPA activities, and monitor their use in the same manner as for RIPA authorised activities.

It should be noted that such NON-RIPA activities would be undertaken at the Authority's own risk, as they are not afforded the legal protections noted in section 4 of this document.

12. OVERSIGHT BY MEMBERS

Elected Members shall have oversight of the Authority's Policy and shall review the Policy annually.

Elected Members shall receive a report on the use of RIPA-regulated activity by officers every ~~three~~ six months.

The report shall be produced by the RMO and presented to the Elected Members (or to such constituted sub-committee as the full Authority shall deem appropriate for oversight purposes) by the RMO and the SRO. The report must not contain any information that identifies specific persons or operations, but must be clear about the nature of the operations carried out and the information obtained.

The RMO and SRO will also report details of any 'Non-RIPA' surveillance in precisely the same fashion.

Following that report, Elected Members may make such amendments as they deem necessary to the Authority's Policy, and may give such directions as they deem necessary to the RMO and SRO in order to ensure that the Policy is followed.

Elected Members may not interfere in individual authorisations. Their function is to review the reports and satisfy themselves that the Policy is robust and is being followed by all relevant officers. Although Elected Members are ultimately accountable to the public for the Authority actions, it is essential that there is no possibility of political interference in investigatory or enforcement operations.

13. ADOPTION OF POLICY AND AMENDMENTS

The~~is~~ Policy and Resources Committee adopted this Policy and P~~the associated p~~rocedure ~~notes were adopted by the City of London Authority~~ on **14th February 2013**, **and approved amendments on 21st January 2016**. This~~ey~~ replaces any previous policy and procedure.

The RMO is instructed to make any changes as are necessary to these documents in order to ensure that they comply with any changes in primary legislation and/or with any codes of practice. Changes made under this section must be reported to Members in the next quarterly report.

The RMO is authorised to amend the list of Authorising Officers in the following circumstances:

- If an Authorising Officer is replaced in their substantive post, the new holder of the post may be added to the list, subject to the training requirement being satisfied.

- If an Authorising Officer fails to attend training or does not meet the required standard, they may be suspended or removed from the list and replaced by another officer of equivalent rank who has attended training and meets the appropriate standard.

- In the case of reorganisation, the RMO may substitute officers of similar rank, always providing that the number of Authorising Officers will not exceed the number approved by Members.

APPENDIX ONE

CITY OF LONDON

LIST OF AUTHORISING OFFICERS (not to exceed four)

POST	**NAME**
Audit Manager	Jeremy Mullins
Head of Audit & Risk Management	Paul Nagle
Director, Port Health & Public Protection Director (Markets & Consumer Protection)	Jon Averns

LIST OF DESIGNATED PERSONS REGISTERED WITH NAFN OR FOR APPROVING THE ISSUE OF A NOTICE IN RESPECT OF ACCESS TO COMMUNICATIONS DATA (not to exceed four)

POST	**NAME**
Audit Manager	Jeremy Mullins
Head of Audit & Risk Management	Paul Nagle

SINGLE POINT OF CONTACT FOR ACCESSING COMMUNICATIONS DATA

POST	**NAME**
Senior Investigator	Chris Keesing

IMPORTANT NOTES

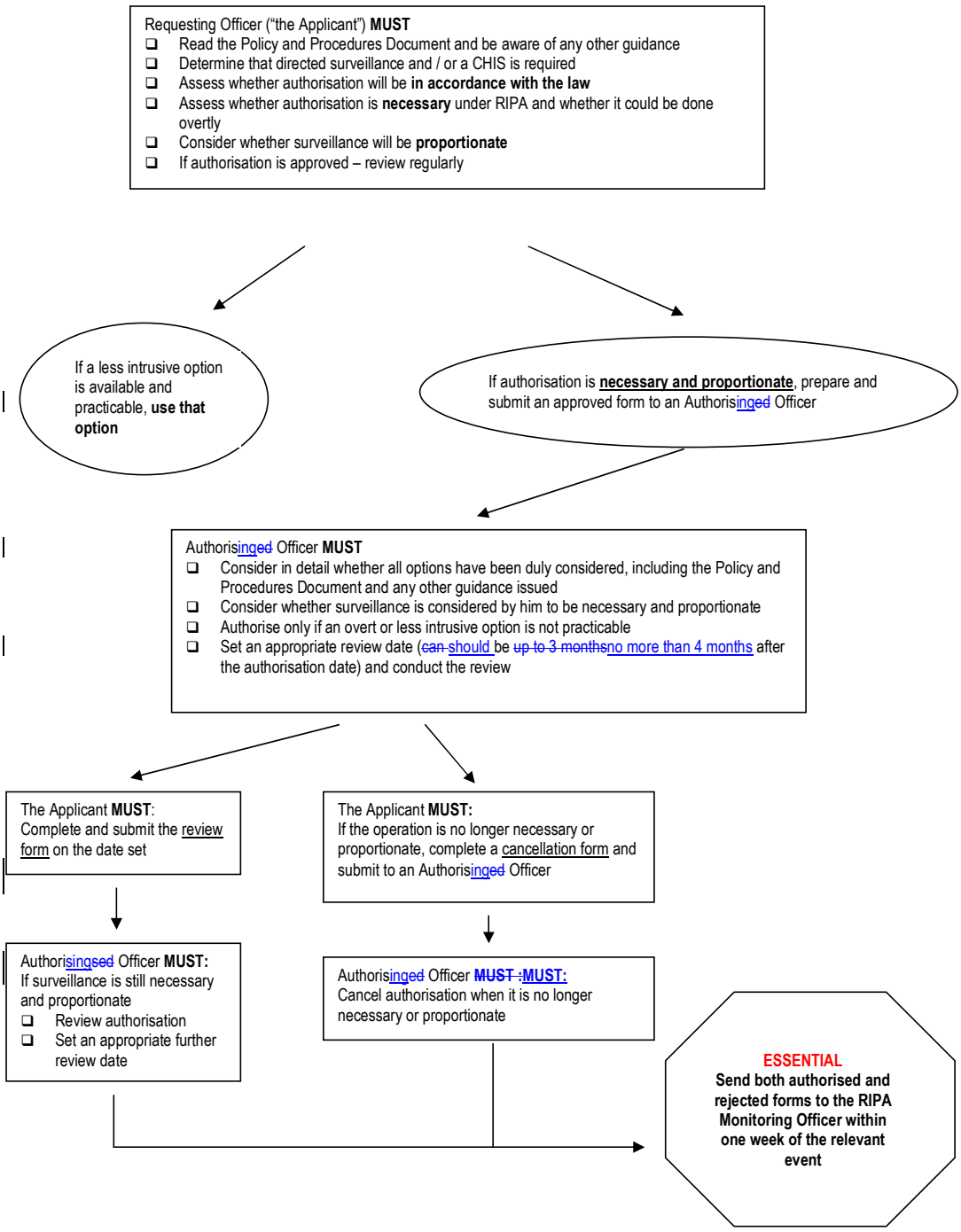
A. Even if a post is identified in the above list, the persons currently employed in such posts are not authorised to sign RIPA forms unless: (i) certified by the *RIPA Monitoring Officer* to do so and, (ii) NAMED in the list.

B. Only the Town Clerk and Chief Executive (as Head of the Paid Service) or, in his absence, the person acting as Head of the Paid Service is authorised to sign forms relating to Juvenile or Vulnerable Individual CHIS' and/or where confidential information, including legally privileged information, is likely to be acquired.

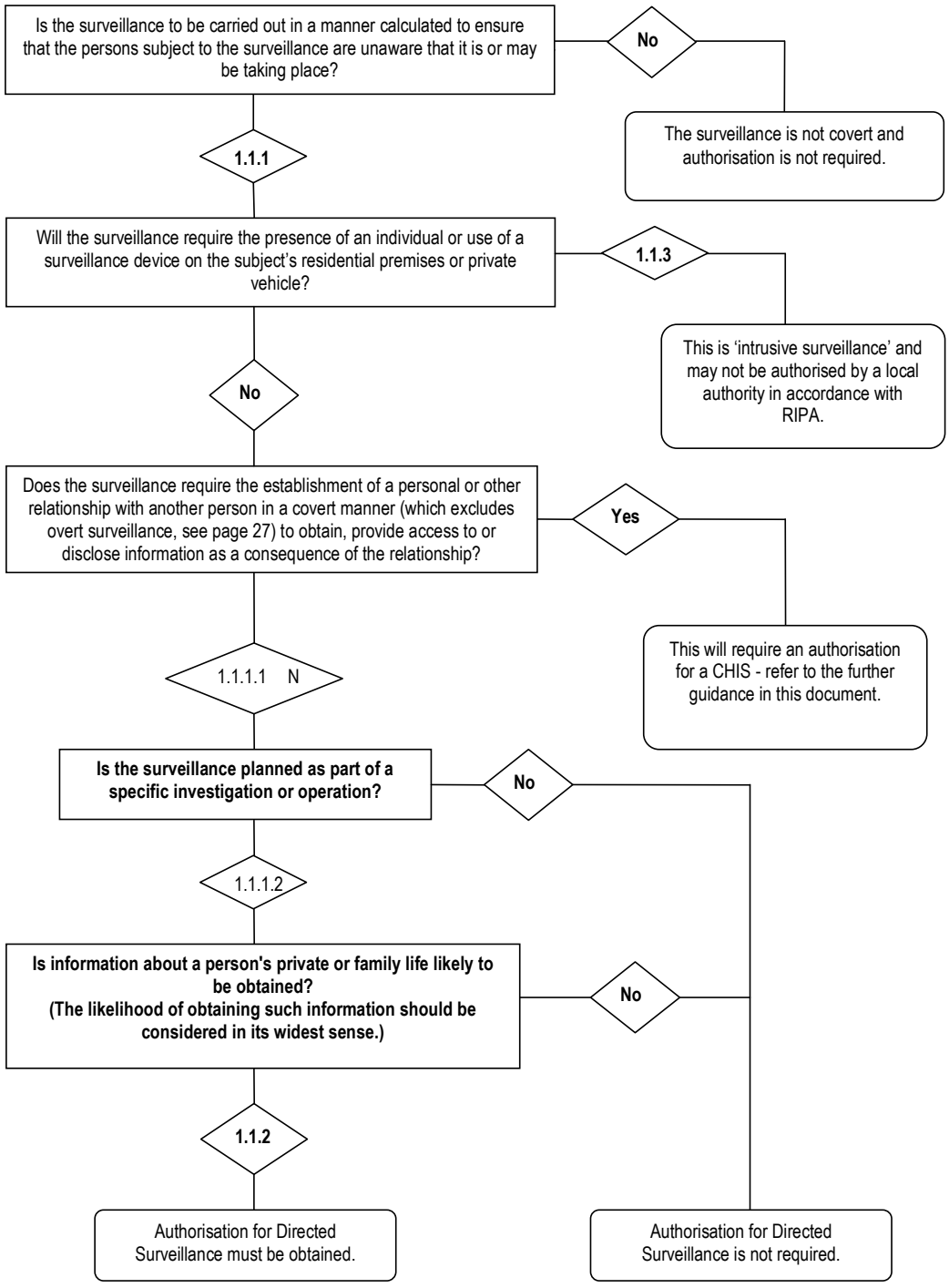
C. If a Head of Service wishes to add, delete or substitute a post, they must refer such a request to the *RIPA Monitoring Officer* in advance for consideration.

APPENDIX TWO

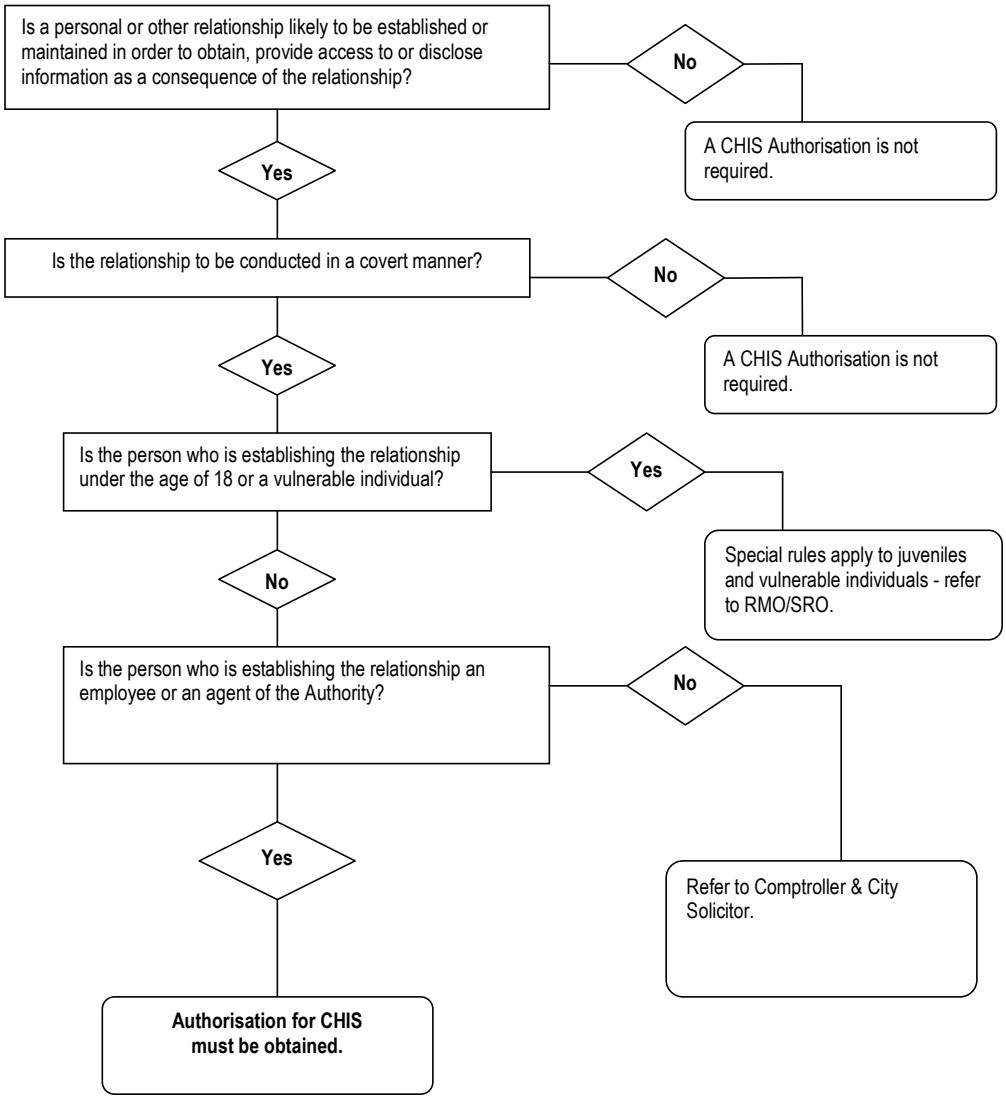
RIPA FLOW CHART FOR DIRECTED SURVEILLANCE AND CHIS



Determination whether DS authorisation is required



Determination whether CHIS authorisation is required



APPENDIX THREE

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 :

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

- The full text of the Codes of Practice are available here :

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

- The Act is available here :

http://www.legislation.gov.uk/ukpga/2000/23/contents

- The Office of Surveillance Commissioners website has some useful information and advice and is available here :

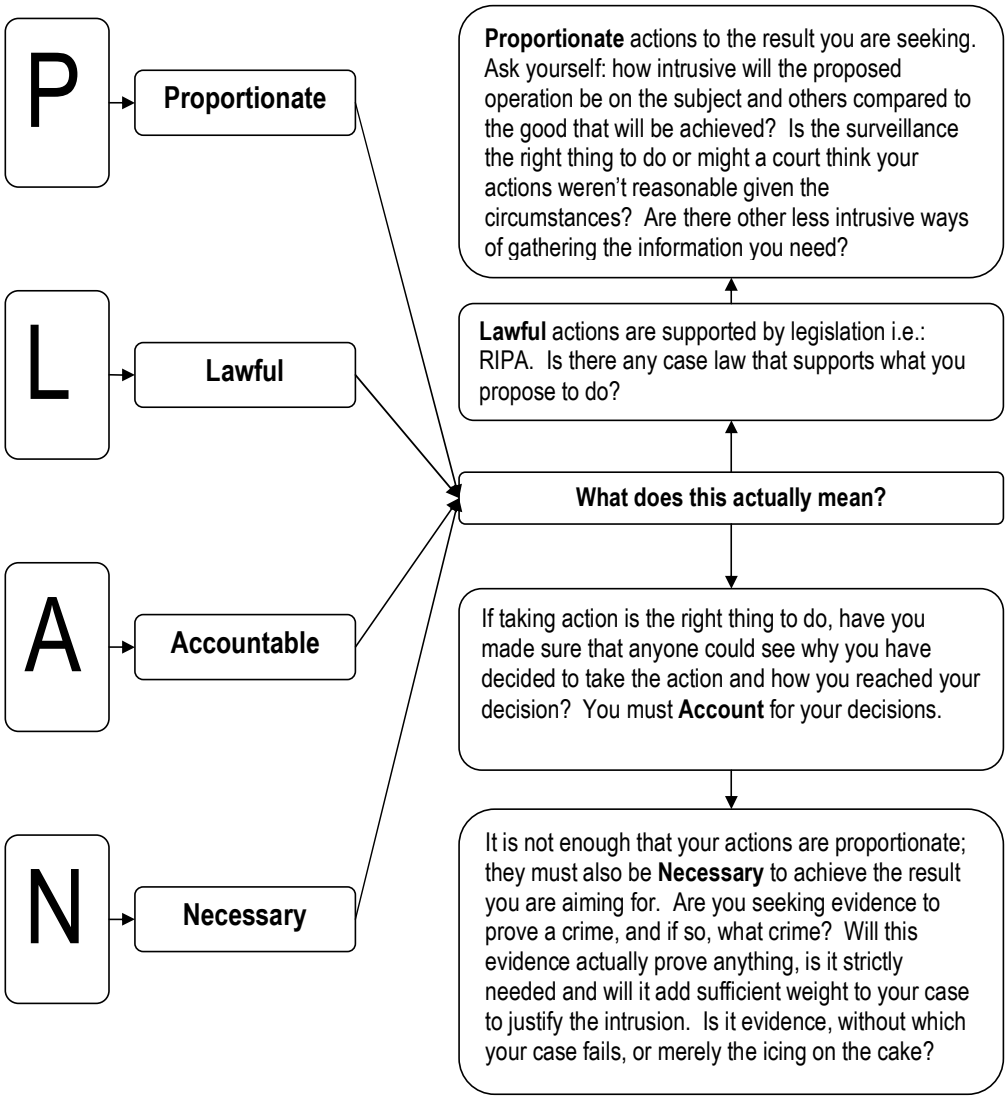
http://surveillancecommissioners.independent.gov.uk/

- You can ask for advice from ITS Training by emailing help@its-training-uk.com . This is a free service to investigation officers only.

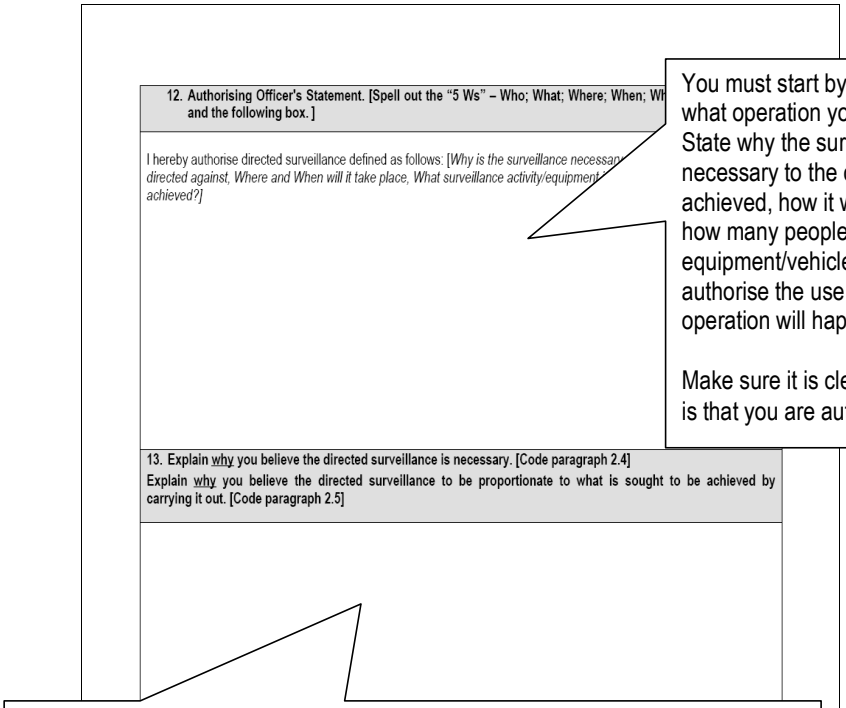
If you have any problems accessing these links, you must report this immediately to the SRO.

APPENDIX FOUR

Notes for Guidance for Authorisation – Directed Surveillance



Authorising Officer's Statement



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.

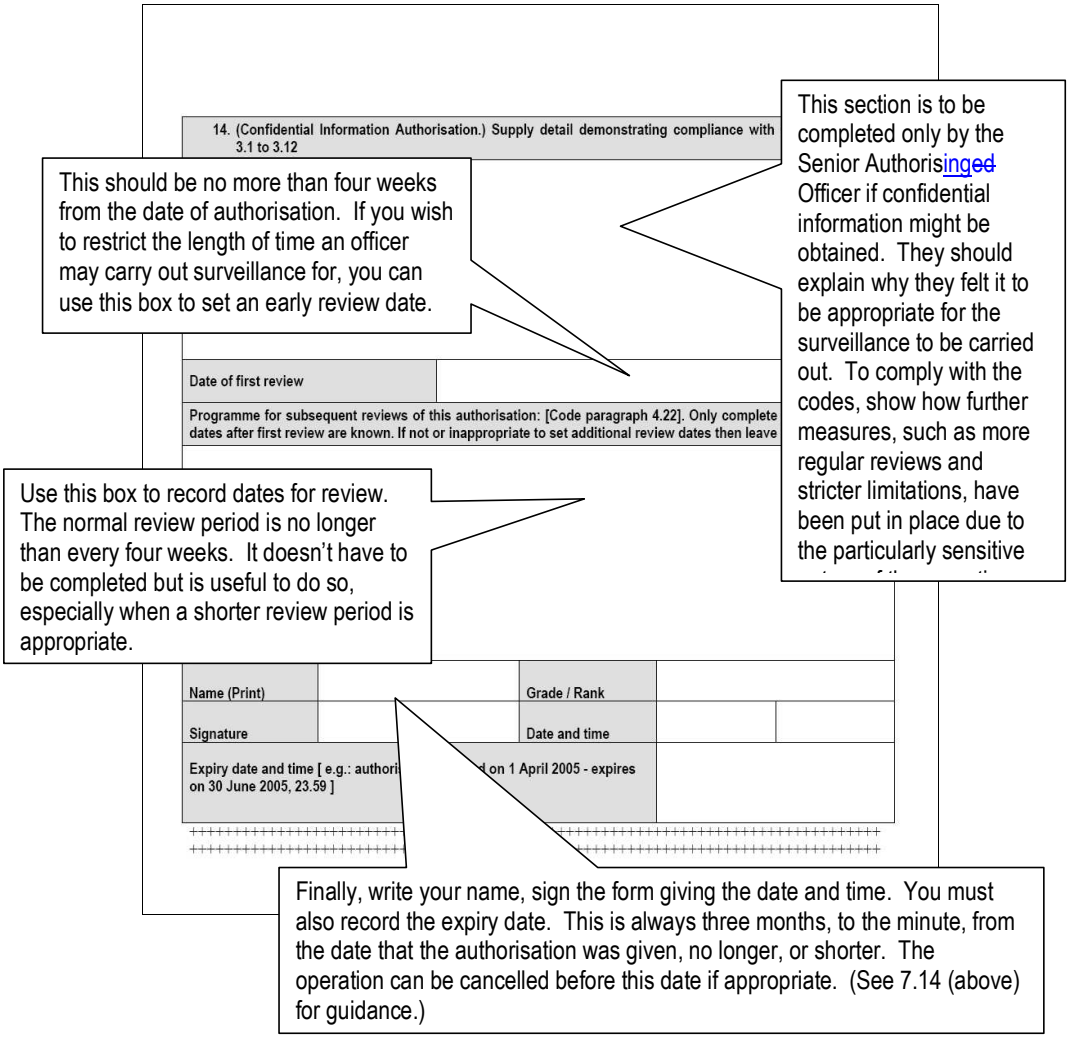
Now you must explain your decision. Simply stating that you "agree with the officer who applied for the reasons they gave" is not acceptable. You must give, in your own words, a detailed account of how you came to decide that the operation was necessary and proportionate. Make sure that you review the 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 target'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 the offence 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.

Authorising Officer's Statement



~~Sections 15 and 16:~~

~~These sections relate to oral authorisations that may be granted or renewed only in urgent cases. If 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 FIVE

Checklist – Can the Authority use RIPA?

Authorisation will be required for a proposed activity if the answer is **'Yes'** to all of the following questions.

If the answer is **'No'** to any of the following questions, the proposed activity falls outside the scope of RIPA.

1. Is the proposed activity 'surveillance'?

The Officer must decide whether the proposed activity will comprise monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording anything monitored, observed or listened to in the course of the proposed activity and whether a surveillance device will be used.

2. Is it 'covert'?

The Officer must decide whether the proposed activity will be carried out in a manner calculated to ensure that the target(s) will be unaware that it is or may be taking place.

3. Is it 'directed'?

The Officer must decide whether the proposed activity is for the purposes of a specific investigation/operation.

4. Is it likely to result in obtaining private information about this person?

The Officer must decide whether any information about the target /targets' private or family life is *likely* to be obtained. This test is different from: "Is there the faintest chance that I will obtain private information?"

5. Is it a 'foreseen/planned response'?

The Officer must decide whether the proposed activity is something other than an immediate response to events. If the proposed activity has been planned in advance and is not just an immediate reaction to events happening in the course of the Officer's work, it is not unforeseen and requires authorisation if all the answers to questions 1 to 4 have also been 'Yes'.

6. Is it a 'Core Function' of the Authority?

RIPA applies to investigations relating to one of the 'Core Functions' of the Authority – that is, matters which relate to functions the Authority is required to carry out as a local authority (such

as investigating benefit fraud or looking into allegations of fraudulent subletting). If the investigation is an 'ordinary function' of the Authority (such as those involving disciplinary matters allegations of fake sickness or theft from the stationary cupboard, which would lead to internal disciplinary action) RIPA does not normally apply. This Authority will nevertheless require RIPA-compliant procedures to be considered in all non-Core Function investigations.

APPENDIX SIX

The Role of the *RIPA Monitoring Officer (RMO)*

The RIPA Coordinator for the Authority is the Authority's *RMO*.

Phone: **External: 020 7332 ~~1409~~3327** **Internal: ~~1409~~ 3327**

Email: neil.davies@cityoflondon.gov.uk ~~lorraine.brook@cityoflondon.gov.uk~~

The *RIPA Monitoring Officer* will maintain a register centrally of all authorisations, grants, refusals, reviews, renewals and cancellations. The role of the RMO includes: -

- Reviewing decisions and raising concerns with Authorising Officers (AOs).
- Arranging three or four monthly moderation meetings between AOs so that they can ensure consistency of approach.
- Arranging training and refreshers.
- Keeping records of those allowed to grant authorisations.
- Removing people from the List if the Policy/Code are not followed/training skipped etc.
- Checking for updated advice (OSC website etc.).
- Drawing to Head of Paid Service and Leader's notice of potential problems.

Each Authorising~~ed~~ Officer is personally responsible for reporting the following information to the *RIPA Monitoring Officer* as soon as possible and, in any event, within one working day: -

- Authorisation of DS/CHIS.
- Review of DS/CHIS.
- Renewal of DS/CHIS.
- Cancellation of DS/CHIS.
- Any unexpected deviations from normal practice or procedure.
- Any unauthorised surveillance operations.
- Any surveillance authorised outside of RIPA.
- Any other matter concerning the authorisation of surveillance that may harm the Authority's interests.

The *RMO* will keep the records for three years to comply with Home Office Guidance.

The Authorising~~ed~~ Officer should also keep the following: (although there is no requirement for this to form part of the Central Register maintained by the RIPA CMO):

- a copy of the application, authorisation and supplementary documentation and notification of approval given by the Authorising~~ed~~ Officer;
- a record of the period over which the surveillance has taken place;
- frequency of reviews prescribed by the Authorising~~ed~~ Officer;

- a record of the result of each review of an authorisation;
- a copy of any renewal of an authorisation, and supporting documentation submitted when it was requested; and
- the date and time any instruction was given by the Authorising~~ed~~ Officer.

Records must be retained in accordance with Data Protection laws and codes of practice.

Storage of Authorisation Forms

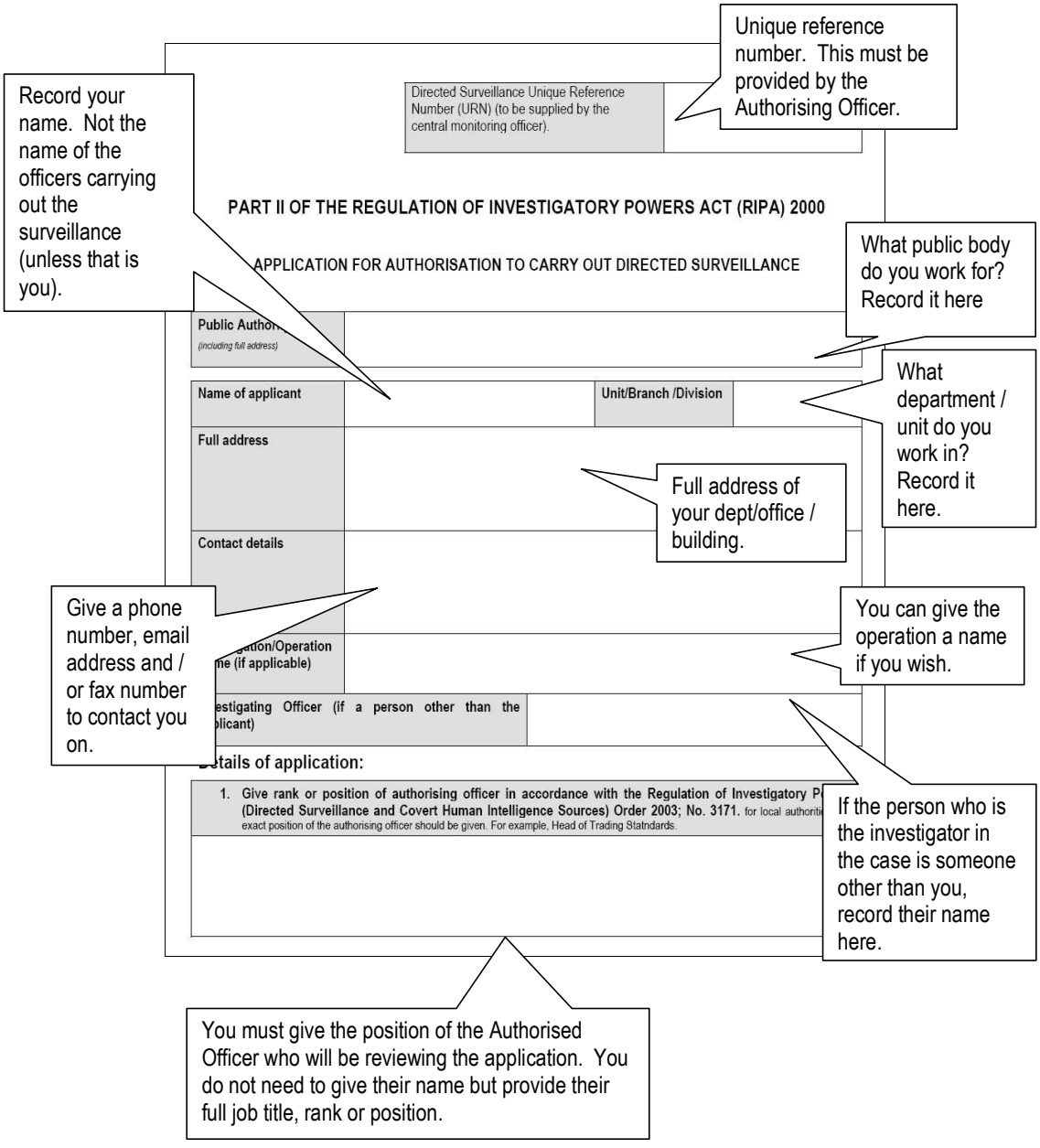
The Policy makes each Director responsible for organising sufficient systems within their service.

The original forms must be retained on the investigation file. Copies must be retained by both the Authorising Officer and the RMO with the Central Monitoring Record. The *RMO* must be sent a notification, **within two working days,** of all grants, refusals, reviews, cancellations and renewals of authorisations to satisfy Home Office Code of Practice recommendations.

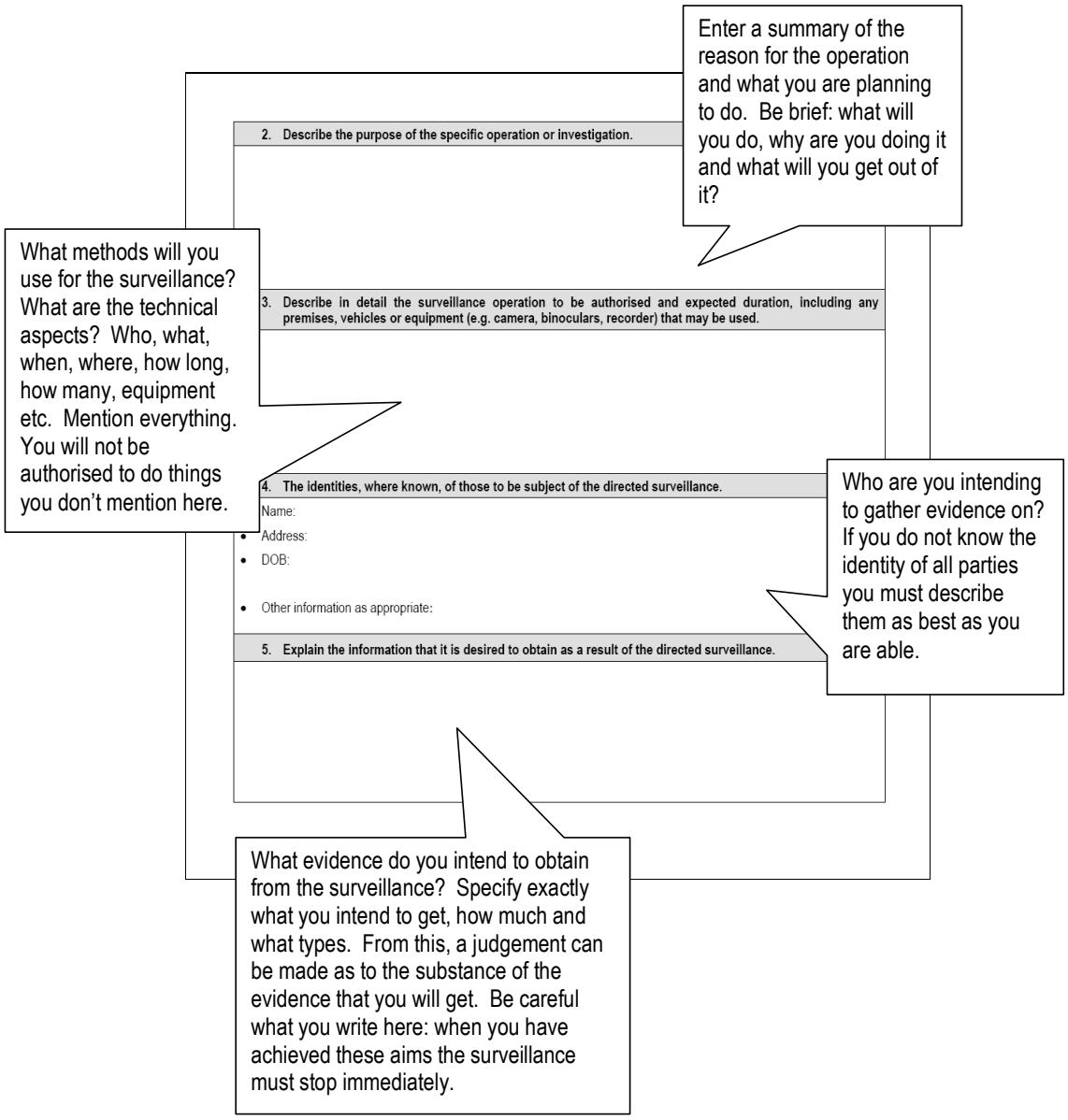
The *RMO* will retain records for at least three years after the completion of the investigation. All officers are reminded of Data Protection requirements about retention and storage of documents. If in doubt, advice must be sought from the RMO.

APPENDIX SEVEN

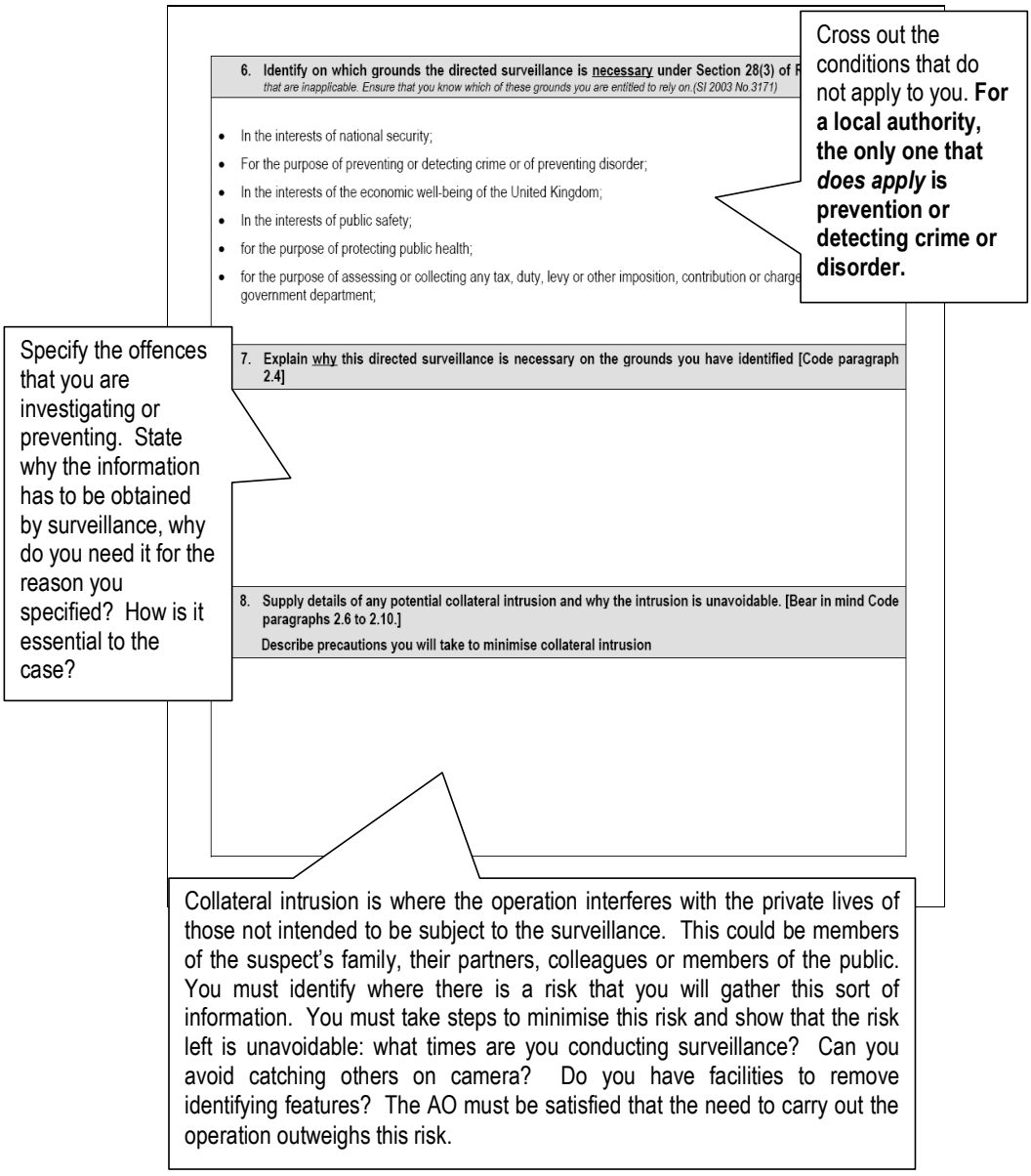
The RIPA 1 Form – Guidance Notes on Completion



Page Two


2. Describe the purpose of the specific operation or investigation.
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?
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.
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.
4. The identities, where known, of those to be subject of the directed surveillance.
Name:
Address:
DOB:
Other information as appropriate:
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.
5. Explain the information that it is desired to obtain as a result of the directed surveillance.
What evidence do you intend to obtain from the surveillance? Specify exactly what you intend to get, how much and what types. From this, a judgement can be made as to the substance of the evidence that you will get. Be careful what you write here: when you have achieved these aims the surveillance must stop immediately.

Page Three



6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of R
that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on.(SI 2003 No.3171)

- 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
government department;

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]
Describe precautions you will take to minimise collateral intrusion

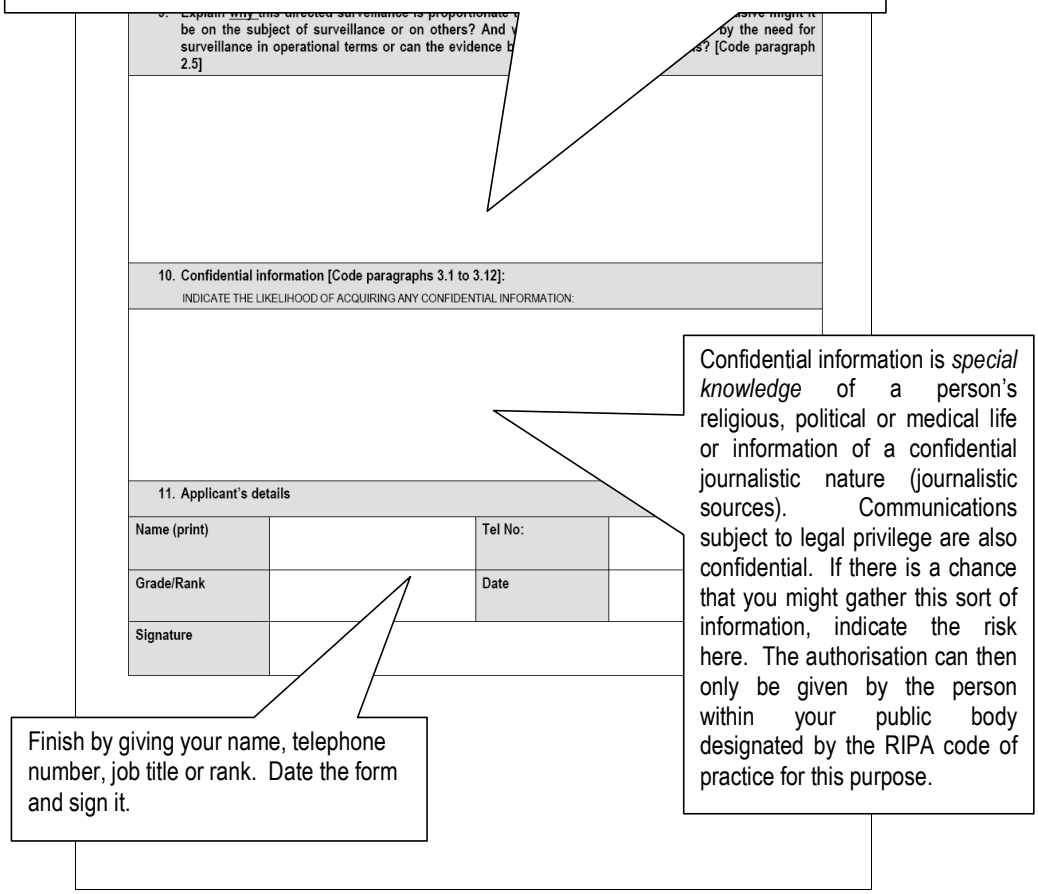
Cross out the conditions that do not apply to you. **For a local authority, the only one that *does apply* is prevention or detecting crime or disorder.**

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?

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.

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 will 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?



be on the subject of surveillance or on others? And y … by the need for surveillance in operational terms or can the evidence b … s? [Code paragraph 2.5]

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.