Regulation of Investigatory Powers Act 2000 (RIPA)

Policy and Procedures

What is RIPA?

The Regulation of Investigatory Powers Act (RIPA) is concerned with the regulation of surveillance by public authorities in the conduct of their legitimate business. Surveillance is an unavoidable part of modern public life, but in the past had not been the subject of formal statutory control. The RIPA was enacted to regularise that position and to ensure that, in conducting surveillance, public authorities have regard to The Human Rights Act 1998 and to Article 8 of the European Convention on Human Rights - the right to a private and family life.

The use of surveillance is an interference with rights protected by Article 8 of the European Convention on Human Rights unless the interference is in accordance with the law, is in pursuit of one or more of the legitimate aims established by Article 8(2) and is 'necessary in a democratic society',

RIPA is only appropriate for surveillance, which relates to the "core functions" of the Council and is for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco (the crime threshold) and where it meets home office requirements.

All RIPA authorisations require Magistrate approval.

What RIPA is not

General observation forms part of the duties of some Council officers. Environmental Health and Planning Officers might covertly observe and then visit premises as part of their enforcement function. Such observation may also involve the use of equipment merely to reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday functions of law enforcement. These are not constrained by RIPA. RIPA also does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property. This low-level activity will not usually be regulated by RIPA.

The Council's overarching approach to the use of RIPA

Because of the potential interference with rights protected by Article 8 of the European Convention on Human Rights, the Council's guiding principle is that the use of covert surveillance techniques or the use of a covert human intelligence source ('CHIS') should only occur:

(i) rarely;
(ii) in exceptional circumstances;
(iii) as a last resort;
(iv) to prevent or detect crime (subject to the crime threshold) or prevent disorder and **for no other purpose whatsoever.**

Further guidance can be found both in the 2014 Home Office Publications and the OSC Procedures and Guidance.

Any Investigating Officer considering making an application should first consult with the Senior Responsible Officer.

What forms of surveillance can be carried out?

The Council is entitled to authorise covert directed surveillance and to use Covert Human Intelligence Sources (informants), known as CHIS. **The Council is not allowed to authorise and must not carry out Intrusive Surveillance.** Intrusive surveillance is covert (undercover) surveillance relating to anything taking place on residential premises or in a private vehicle. The surveillance is intrusive if it involves the presence of either an individual, or a surveillance device, on the premises or in the vehicle.

- **Directed Surveillance** is where the surveillance is not intrusive and is undertaken for the purposes of a specific investigation or a specific operation in such a manner as is likely to result in the obtaining of private information about a person

- **Covert Human Intelligence** is where undercover officers or informants are used to obtain information. A person is a covert human intelligence source if he/she develops a relationship with another person in order to covertly obtain information or to provide access to information to a third party or to covertly disclose information obtained by the use of such a relationship and the other person is unaware of the purpose of the relationship.

Covert surveillance of Social Networking Sites

The use of the internet and, in particular, social networking sites, can provide useful information for Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the council – for example Fraud, Planning Enforcement, Licensing or Environmental Health, but will equally apply to some non-enforcement teams, such as Debt Collection or Housing.

The use of the internet and social networking sites may potentially fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy).

Further guidance on the use Social Networking Sites is given in Section 289 of the OSC Procedures and Guidance in also at Appendix 3.

Acquisition and Disclosure of Communications Data

The Council has powers to acquire communications data. There are certain safeguards that apply in relation to the acquisition of such data. It has to be demonstrated that it is necessary for the purpose of **preventing or detecting crime or preventing disorder**; and proportionate to what is sought to be achieved by acquiring such data. If collateral intrusion is envisaged it must be demonstrated that the intrusion is justified.

The procedure is similar to that for the authorisation of directed surveillance and covert human intelligence but has extra provisions and processes.

The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to the exercise of the powers under RIPA. The mechanism for obtaining communications data creates a system of safeguards under a detailed regulatory and legal framework. This ensures that the interference with the right of privacy of an individual through the acquisition of communications data

is necessary and proportionate in any given case.

Further guidance on the **Acquisition and Disclosure of Communications Data** is given at Appendix 4

Who can authorise RIPA surveillance?

The Council has appointed authorising officers of suitable seniority to grant surveillance authorisations for individual incidents (see Appendix 2):

- **Directed surveillance** will only be carried out with the express authority of the authorising officers.

- **Covert Human Intelligence Sources.** Only **a Joint Chief Executive** can authorise the use of Covert Human Intelligence Sources.

- **Acquisition and Disclosure of Communications Data** - Only **a Joint Chief Executive** can authorise the Acquisition and Disclosure of Communications Data**.**

Records of authorisations will be kept centrally by the Senior Responsible Officer and will be monitored and reviewed on a regular basis by Overview and Scrutiny Committee.

Any request received from external authorised agencies, such as the police or security services either to disclose communications data, e.g. billing information, e-mail addresses, etc, or to unlock encrypted data or provide the key to unlock encrypted data, will be referred to a **Joint Chief Executive** who has the power to authorise such requests.

Each Authorising Officer will be responsible for ensuring that copies of any necessary forms are forwarded to the Senior Responsible Officer and that investigating officers are not acting unlawfully. They should ensure they keep a record of requests as a control.

The context for RIPA authorisations

Authorisation to conduct covert surveillance and/or to use a covert human intelligence source will only be given where the Authorising Officer believes that it is necessary for a specific statutory reason as defined by sections 27-29 of the Act and where the Authorising Officer is satisfied that all other means of obtaining evidence have been exhausted. The authorisation will be necessary if the covert surveillance is for the purpose of preventing or detecting crime (subject to the crime threshold) or of preventing disorder and if there is no other means available to the investigating officers.

If the Authorising Officer is satisfied that the action is necessary the Authorising Officer must then go on to consider whether the form and level of proposed surveillance is proportionate to the desired outcome. The term 'proportionate' is used here in the context of the Human Rights Act which requires interference with a human right to be kept to the absolute minimum. Where there is interference it should be measured against the desired outcome. Interference with human rights is only acceptable where the matter being investigated is significant and it is in the public interest to achieve an outcome.

In determining whether an interference is proportionate the Authorising Officer must have regard to issues such as collateral intrusion and the obtaining of confidential information. Collateral intrusion is interference with the human rights of persons other than the subject. The Authorising

Officer must weigh the extent to which the human rights of third parties are infringed and whether such infringement is both necessary and proportionate in the context of the issue being investigate.

Authorising Officers must also assess the extent to which confidential information about the subject will come into the Authority's possession as a result of the investigation. Such information may be relevant to the investigation but protected for example as a result of legal professional privilege or it may be irrelevant but sensitive information, for example medical records. Deliberately obtaining (or the use of) confidential information may only be authorised by a **Joint Chief Executive.**

Finally, the Authorising Officer must give due consideration to the impact on the community of the use of covert surveillance methods. In particular the officer will have regard to community confidence. The Authorising Officer should consider if the circumstances of the investigation were to become public, what the reaction of the community is likely to be and whether and to what extent the Authority would be able to justify the use of its chosen methods.

Quick Checklist

A 'Quick Checklist' is attached at Appendix 3. It should be used before any authorisation application is sought and will determine when any RIPA authorisation is required. If the answer is 'Yes' to all Checklist questions that RIPA approval is required. If the answer is 'No' to any of the Checklist questions, the proposed activity falls outside the scope of RIPA and this policy.

Process for obtaining Authorisations

- All requests for an authorisation to conduct covert surveillance must be submitted by an investigation officer or appropriate manager to the Authorising Officer in writing using the appropriate form. The most up-to-date versions of Forms and Codes of practice must be used.

- Whatever the nature of the decision taken by the Authorising Officer, the decision should be confirmed in writing with reasons for the decision. Authorisations will be regularly reviewed in compliance with the legislation and the reasons for extending or terminating them will also be recorded in writing.

- Authorisations must not be allowed to expire. Authorisations must be reviewed regularly or cancelled after surveillance has been completed and recorded appropriately.

- Surveillance must be carried out adhering at all times to written procedures, good practice and health and safety conditions. All officers involved in applying for, authorising or undertaking surveillance must understand the legal requirements set out in RIPA and any respective Codes of Practice. They will personally be responsible for ensuring the propriety of their involvement. All authorisations, notebooks, surveillance logs and other ancillary documentation that relates to surveillance will be maintained to the required standards and retained for three years. All documentation will be volunteered for any management or regulatory inspection on demand.

- The Senior Responsible Officer is responsible for identifying training needs and ensuring adherence to this procedure.

- Wilful disregard of any part of the Regulation of Investigatory Powers Act Code of Practice or of internal procedures will be a breach of the Officer Code of Conduct and will be dealt with accordingly.

- A central record of all authorisations will be kept by the Senior Responsible Officer.

Magistrate Approval

Following the authorisation an application must then be made to a Magistrates Court for a Hearing. All requests to Magistrates must be on the forms as provided in the Code of Practice issued by the Office of Surveillance Commissioners (OSC). Renewals must also be authorised by the Authorising Officer and approved by the Magistrates.

The preference is that the Authorising Officer is in attendance at the Magistrates Court as the Authorising Officer bears the overall responsibility for the application.

Complaints

If anyone has any reason to believe that they have been subjected to unauthorised covert surveillance by the Council, or they are unhappy about any other aspect of the Council's operation under RIPA, they may complain. The Council operates an internal complaints procedure and full details are available on the Council's website www.hart.gov.uk. A complaint can be made in person, by telephone, in writing or by e-mailing: Complaints@hart.gov.uk.

If they are unhappy with the response they can then contact the Local Government Ombudsman but it is important that they complete the Council's Complaints Procedure BEFORE contacting the Ombudsman.

The Regulation of Investigatory Powers Act 2000, (the UK Act) also separately establishes an independent Tribunal[1]. This has full powers to investigate and decide any cases within its jurisdiction. Details of the relevant complaints procedure can be obtained from:
Investigatory Powers Tribunal
PO Box 33220
London
SWLH 9ZQ
Tel: 02007 035 3711
Website address: www.ipt-uk.com

Adoption of Policy and Amendments

This Policy and the associated procedure note was adopted on **20 December 2016**. It replaces any previous policy and procedure.

The Joint Chief Executive, in consultation with the Leader of the Council and the Chairman of Overview and Scrutiny Committee is authorised to make any changes as are necessary to these documents to ensure that they comply with any changes in primary legislation and/or with any codes of practice. The Joint Chief Executive is also authorised to amend the list of Authorising Officers where appropriate.

[1] The Tribunal has power to cancel authorisations and order destruction of information obtained. The Council is under a duty to disclose to the Tribunal all relevant documentation.

Appendices

Appendix 1 - Key Definitions
Appendix 2 - RIPA Authorising Officers
Appendix 3 - Covert surveillance of Social Networking Sites Guidance Note
Appendix 4 - Acquisition and Disclosure of Communications Data
Appendix 5 - Quick Checklist
Appendix 6 - Flow Chart for Directed Surveillance and CHIS
Appendix 7 - Notes for Guidance Authorisations – Directed Surveillance
Appendix 8 - Forms and Codes
Appendix 9 - Authorising Officer Statements
Appendix 10 - The RIPA 1 Form – Guidance on Completion

Appendix 1 – Key Definitions

Serious Crime
Section 93 (4) of the 1997 Act: Involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or the offence is one, for which a person aged 21 years or over with no previous convictions could reasonably expect to receive a sentence of three years imprisonment or more.

Confidential personal information
Section 99(1) of the 1997 Act: Personal information which a person has acquired or created in the course of any trade, business, profession or other occupation, and which he holds in confidence; and communications as a result of which personal information is acquired or created and held in confidence.

Personal information
Section 99(2) of the 1997 Act: Information concerning an individual (living or dead) who can be identified from it and relating to his physical or mental health or to spiritual counselling or assistance given or to be given to him.

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

Communications data
Any information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories: -
21(4)(a) Traffic data - where a communication was made from, to whom and when
21(4)(b) Service data– use made of service e.g. Itemised telephone records
21(4)(c)) Subscriber data – information held or obtained by operator on person they provide a service to.

Surveillance
Section 48(2) of RIPA:
- monitoring, observing, listening to persons, their movements, conversations, other activities or communications
- recording anything monitored, observed or listened to in the course of surveillance
- surveillance, by or with, assistance of a surveillance device.
- Surveillance can be
- directed
- intrusive.

Directed surveillance
Section 26(2) of RIPA: Covert, but not intrusive, and undertaken
- for a specific investigation or operation
- in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation); and
- not as an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable eg spotting something suspicious and continuing to observe it.

Intrusive
Section 26(3) of RIPA: Only if covert and
- carried out in relation to anything taking place on residential premises or in a private vehicle; and

- involves the presence of an individual on the premises or vehicle or is carried out by a surveillance device.

Private information
Section 26(10) of RIPA: In relation to a person, includes any information relating to his private or family life.

[It is helpful to have regard to the judgment in the case of Amann v Switzerland Feb 2000. In relation to Article 8 it said ***"….respect for private life comprises the right to establish and develop relationships with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature".***]

Covert Human Intelligence Source (CHIS)
Section 26(8)(a)-(c) of RIPA: A person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that

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

Conduct and use of a CHIS
Section 26(7)(a)(b) of RIPA:

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

Appendix 2 – RIPA Authorising Officer

Joint Chief Executives – Communications Data, Directed Surveillance and Covert Human Intelligence

Heads of Service – Directed Surveillance

- Head of Corporate Services
- Head of Environment and Technical Services
- Head of Community Services
- Head of Regulatory Sevices

Appendix 3 – Covert surveillance of Social Networking Sites Guidance Note

In using social media for the gathering of evidence:

- officers must not 'friend' individuals on social networks
- officers should not use their own private accounts to view the social networking accounts of other individuals
- officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation
- further viewing of open profiles on social networking sites to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
- officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

The purpose of this guidance note is to provide clarity on the Council's position:

1. It is not possible to provide a definitive list of social networking sites, so this should be taken to mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether accepted as 'friends' or otherwise. This might include sites such as 'Facebook' and 'Linked-In'

2. As the definition of 'private information' under RIPA includes:

   'any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships'

Sites used to advertise goods and services should be included within the definition. Although there is likely to be a reduced expectation of privacy with this type of site, there is still the possibility of obtaining private information which may be subsequently used in any enforcement proceedings.

1. If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile once in order to take an initial view as to whether there is any substance to the allegation or matter being investigated.

2. The initial viewing must be reasonable – for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual's profile or to print out several pages just in case they may reveal something useful.

3. In some cases where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing. However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.

4. If there is a need to monitor an individual's social networking site, authorisation must be obtained.

5. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by an Authorising Officers and then approved by a Magistrate.

Appendix 4 - Acquisition and Disclosure of Communications Data

Introduction

The Council has powers to acquire communications data. There are certain safeguards that apply in relation to the acquisition of such data. It has to be demonstrated that it is necessary for the purpose of **preventing or detecting crime or preventing disorder**; and proportionate to what is sought to be achieved by acquiring such data. If collateral intrusion is envisaged it must be demonstrated that the intrusion is justified

- The procedure is similar to that for the authorisation of directed surveillance and CHIS but has extra provisions and processes

- The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to the exercise of the powers under RIPA. The mechanism for obtaining communications data creates a system of safeguards under a detailed regulatory and legal framework. This ensures that the interference with the right of privacy of an individual through the acquisition of communications data is necessary and proportionate in any given case.

- Only the Joint Chief Executive can authorise the use of the power to acquire communications data. In addition, all authorisations require Magistrate approval

.

What is 'Communications data'?

Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories: -

21(4)(a) Traffic data - where a communication was made from, to whom and when
21(4)(b) Service data– use made of service e.g. Itemised telephone records
21(4)(c)) Subscriber data – information held or obtained by operator on person they provide a service to

The Council is restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder. Traffic data is not available to the Council

Authorisations

Authorisations can only apply to conduct to which Chapter II of Part I of the Act apply

The authorisation to obtain and disclose communications data is only allowed if:

a) It is **necessary** for any of the purposes set out in Section 22(2) of the Act. (The Council can only authorise for the purpose set out in Section 22(2)(b) which is the purpose of preventing or detecting crime or preventing disorder); and
b) It is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) the Act)

Consideration must also be given to the possibility of collateral intrusion and whether any urgent timescale is justified.

There are two methods by which the information can be sought from the Communications Service Provider: -

A. By **authorisation** in the following circumstances:

i) The postal or telecommunications operator is not capable of collecting or retrieving the communications data
ii) It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
iii) There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

B. By **notice** to the holder of the data to be acquired (s.22 (4)) which requires the operator to collect or retrieve the data.

Service providers are under a duty to comply with the notice if it is reasonably practicable to do so (s.22 (6)-(8)) and non compliance can be enforced to do so by civil proceedings. The postal or telecommunications service providers normally charge for providing this information.

There are standard forms for authorisations and notice. There are also a number of other administrative forms the SPOC is obliged to complete in certain circumstances, although these will not always involve the requesting officer.

Oral authority and grading of requests

Requests for communications data **CANNOT** be granted orally. They must be made in writing. Requests to Communications Service Providers are graded; grade 3 is the response level to public authorities, requests are normally dealt with within 10 working days. Grades 1 and 2 are requests by the emergency services where there is an immediate threat to life or an exceptionally urgent operation, which requires data within 48 hours.

Duration

Authorisations and notices are only valid for one month beginning with the date on which the authorisation is granted or the notice given. A shorter period should be specified if possible.

Renewal and Cancellation

An authorisation or notice may be renewed at any time during the month it is valid using the same procedure as used in the original application, Renewals require judicial approval.. A renewal takes effect on the date which the authorisation or notice it is renewing expires.

The code requires that all authorisations and notices should be cancelled as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant person or telecommunications operator should be informed of the cancellation of a notice. There is no need for judicial approval upon cancellation of a notice.

Appendix 5 - 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.

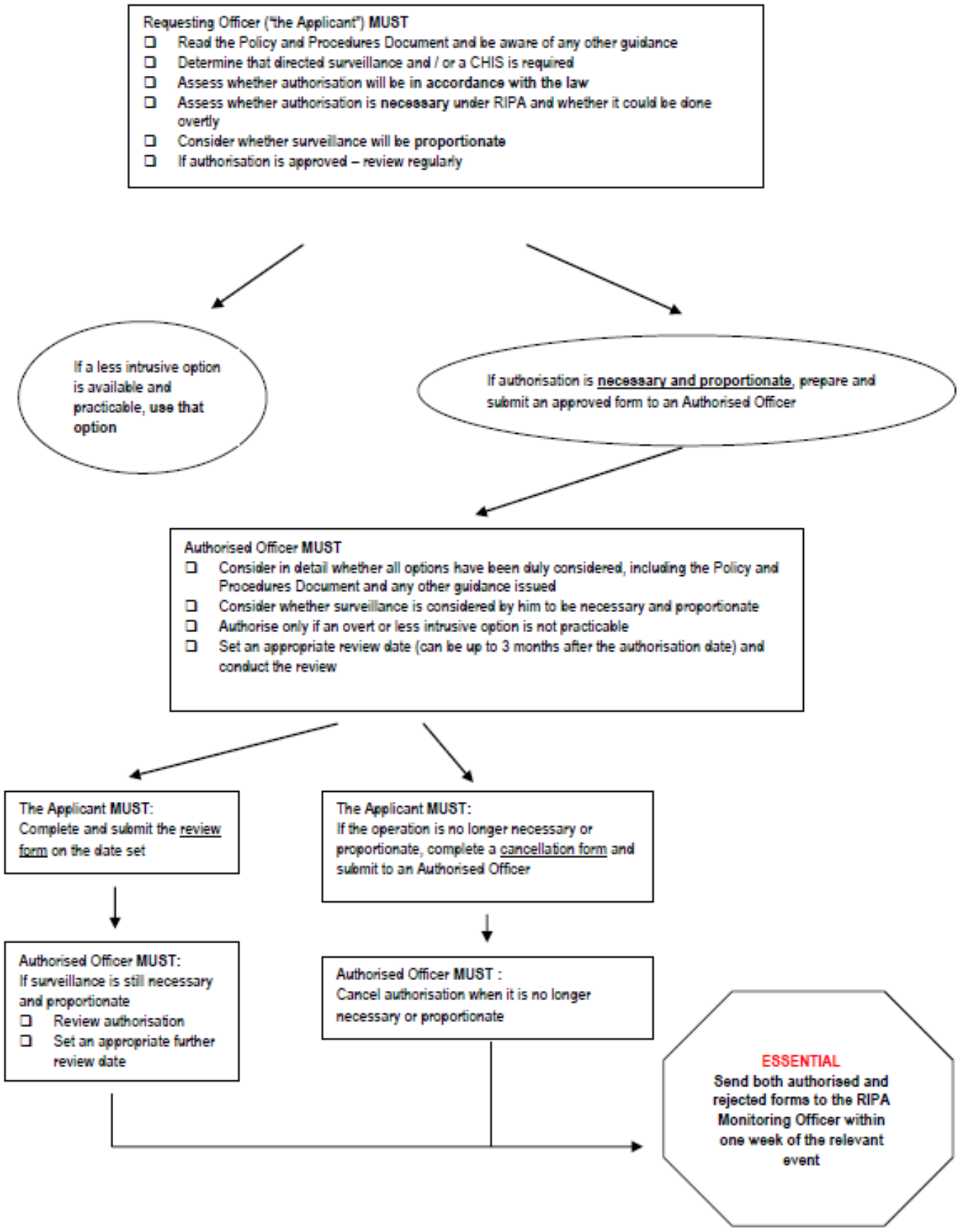
A.4. Is it likely to result in obtaining private information about this person?
☐ information about the target /targets' private or family life is likely to be obtained.

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'.

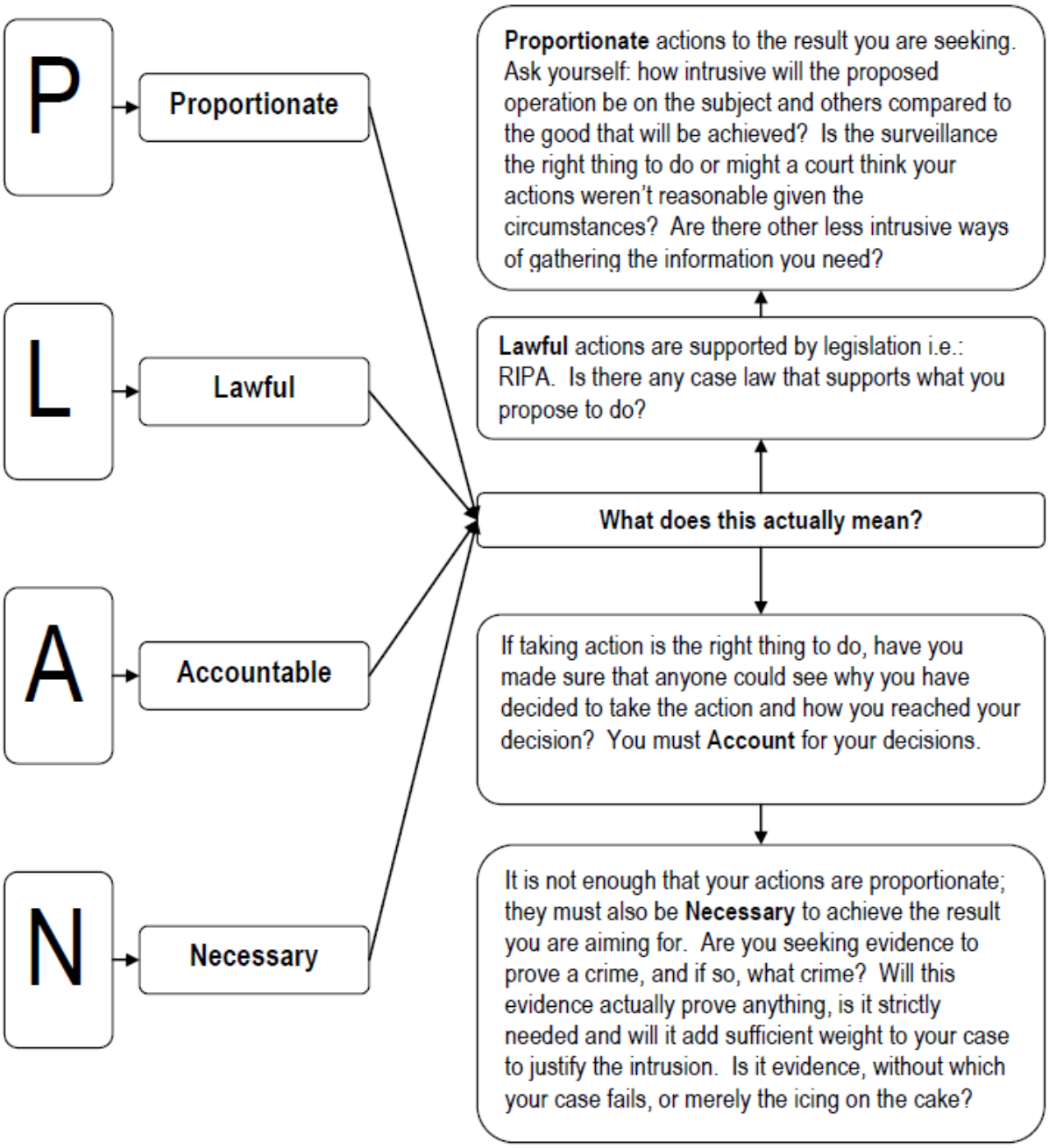
A.6. Is it a "core function" of the Authority?
☐ matters which relate to functions the Authority is required to carry out under statute (such as investigating benefit fraud, planning or food hygiene enforcement, licensing).
☐ is for the purpose of preventing or detecting criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco (the crime threshold)
☐ does it meet Home Office requirements

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

Appendix 6 - Flow Chart for Directed Surveillance and CHIS



Appendix 7 Notes for Guidance for Authorisation – Directed Surveillance



Appendix 8 - Forms and Codes

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, the following links provided access to the currently approved versions.

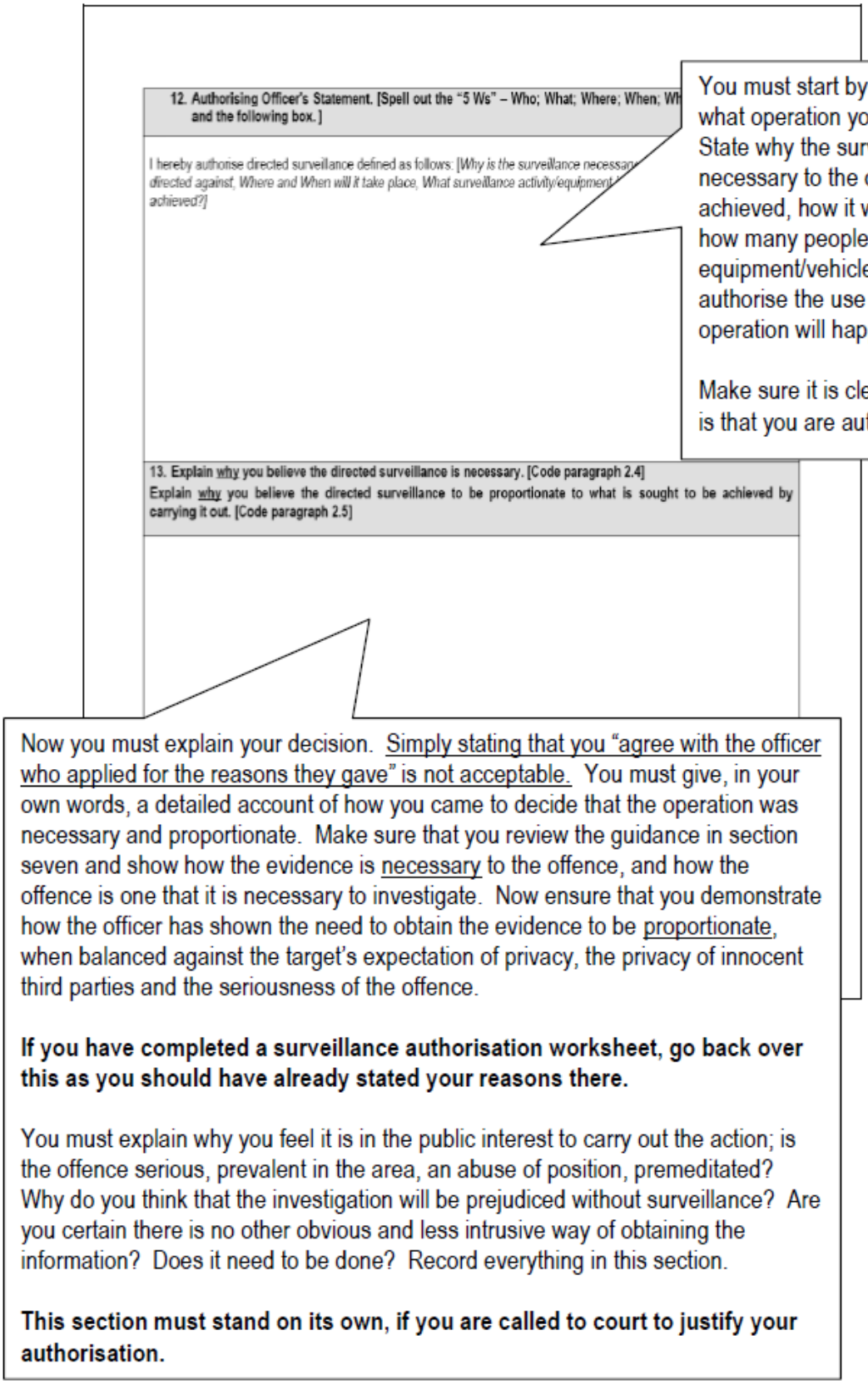
- The most up-to-date RIPA forms must always be used. These are available from the Home Office website: http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

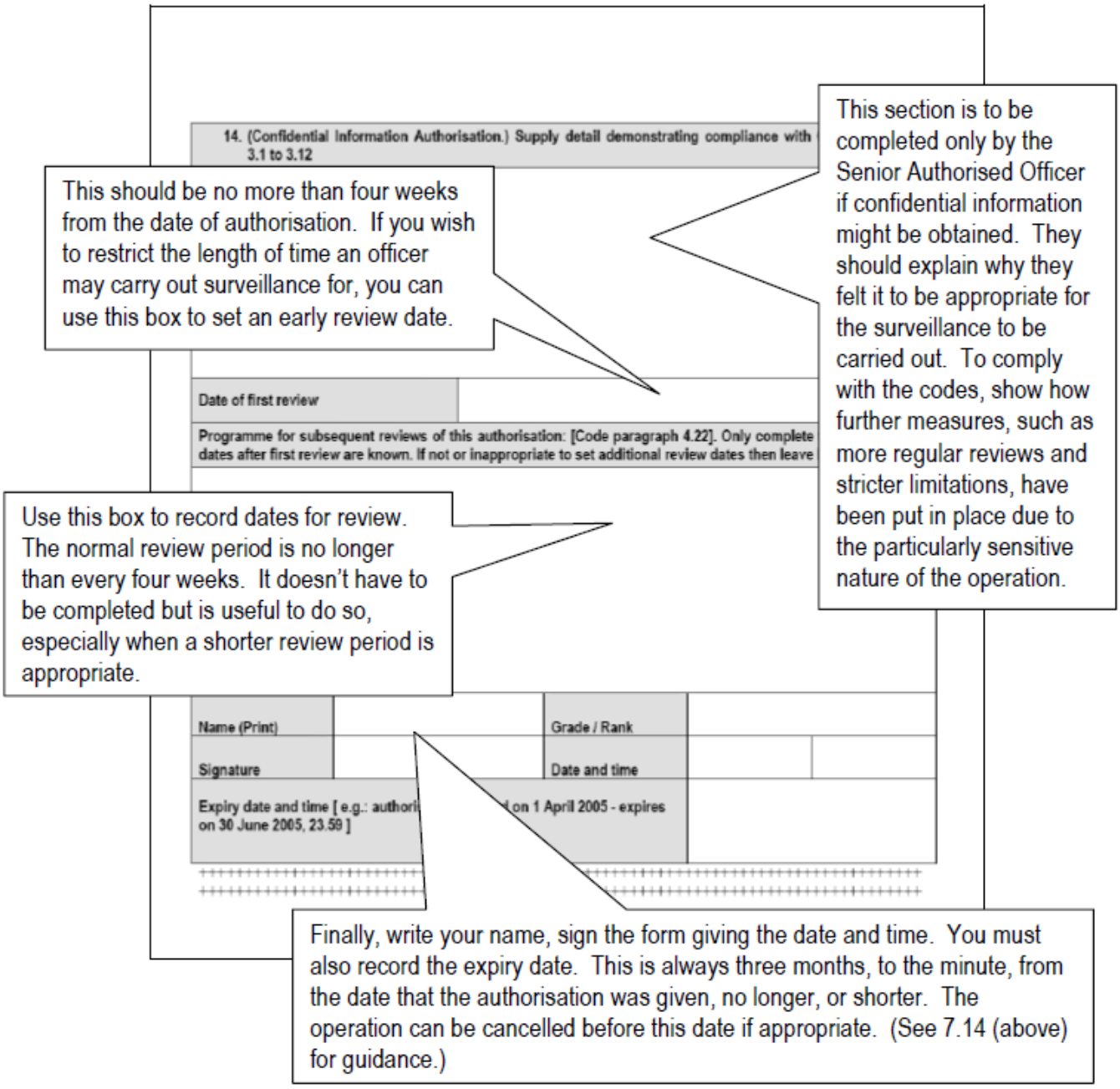
- The full text of the Codes of Practice: http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

- The Act is available here: http://www.legislation.gov.uk/ukpga/2000/23/contents

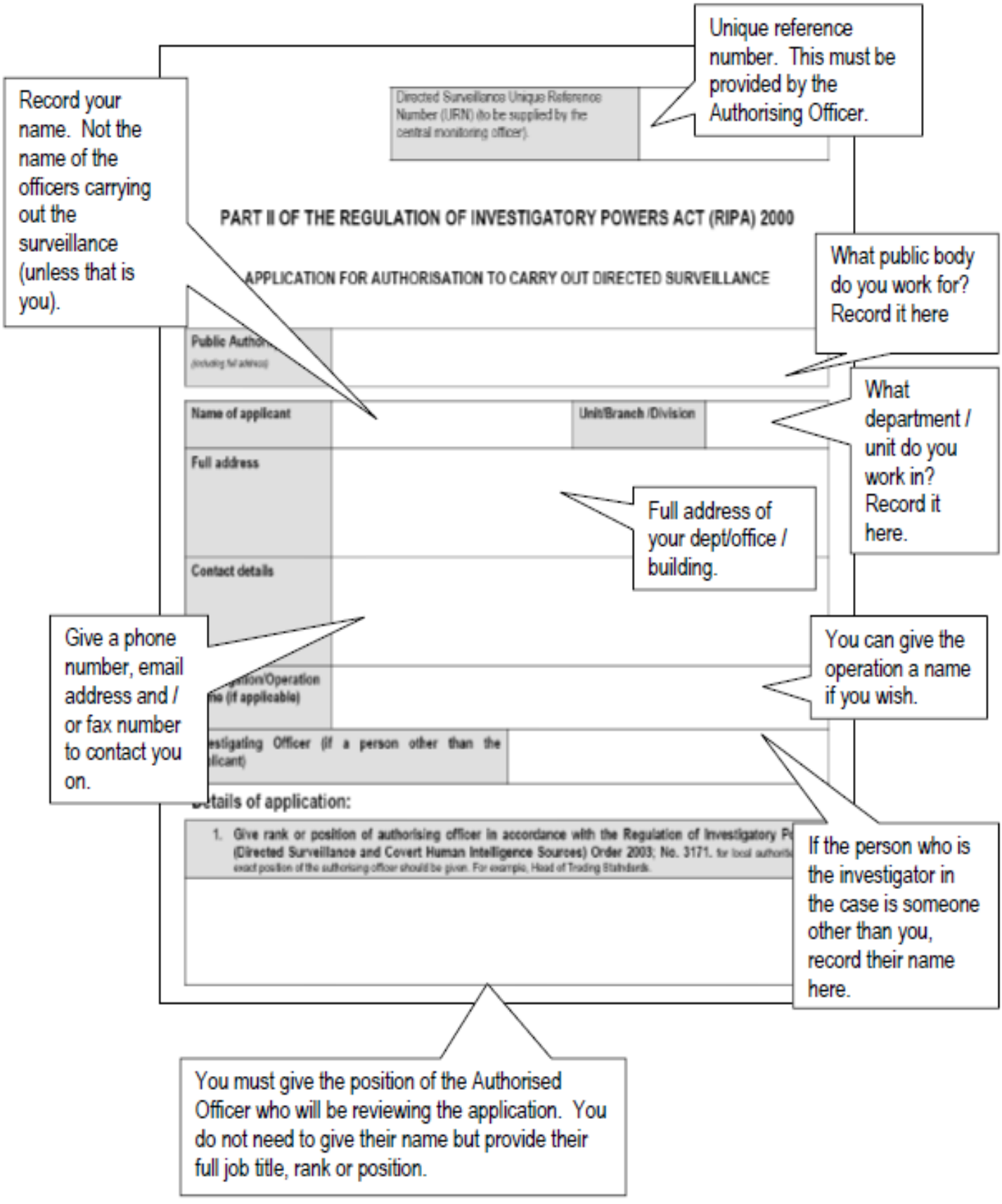
- The Office of Surveillance Commissioners website has some useful information and advice and is available here: http://surveillancecommissioners.independent.gov.uk

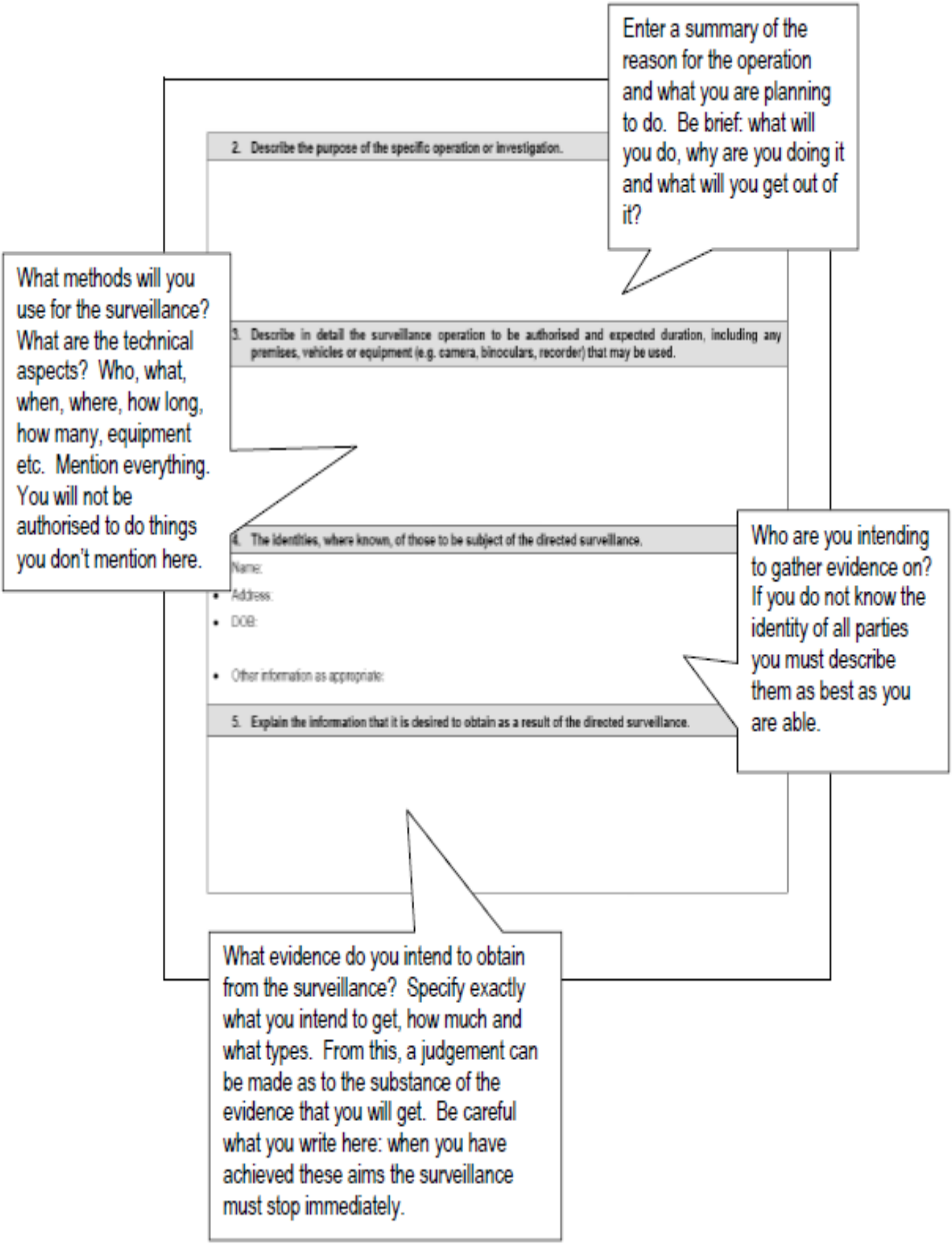
Appendix 9 - Authorising Officer Statement

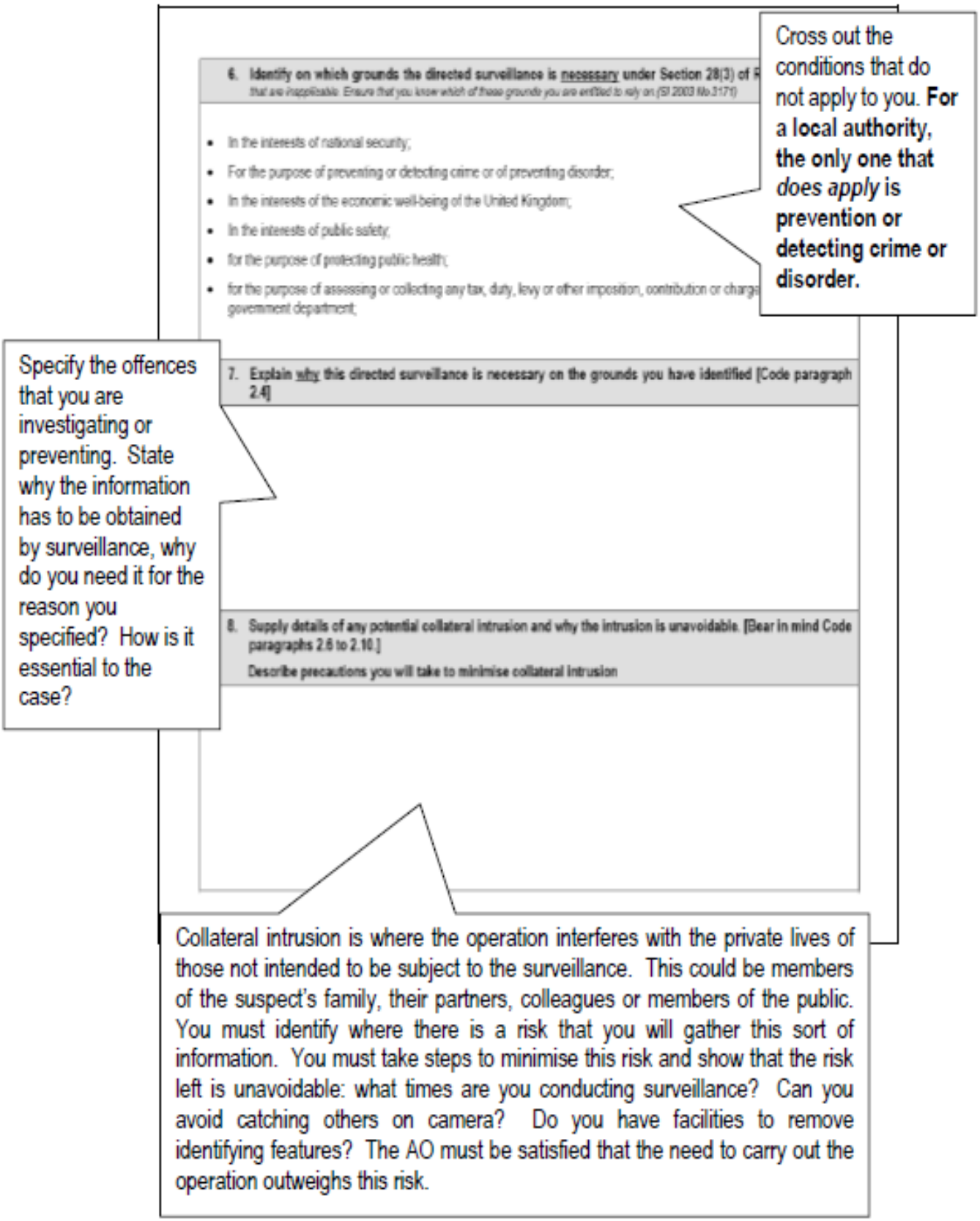



14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with 3.1 to 3.12
This should be no more than four weeks from the date of authorisation. If you wish to restrict the length of time an officer may carry out surveillance for, you can use this box to set an early review date.
This section is to be completed only by the Senior Authorised Officer if confidential information might be obtained. They should explain why they felt it to be appropriate for the surveillance to be carried out. To comply with the codes, show how further measures, such as more regular reviews and stricter limitations, have been put in place due to the particularly sensitive nature of the operation.
Date of first review
Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete dates after first review are known. If not or inappropriate to set additional review dates then leave
Use this box to record dates for review. The normal review period is no longer than every four weeks. It doesn't have to be completed but is useful to do so, especially when a shorter review period is appropriate.
Name (Print)
Grade / Rank
Signature
Date and time
Expiry date and time [e.g.: authori
on 1 April 2005 - expires on 30 June 2005, 23.59]
Finally, write your name, sign the form giving the date and time. You must also record the expiry date. This is always three months, to the minute, from the date that the authorisation was given, no longer, or shorter. The operation can be cancelled before this date if appropriate. (See 7.14 (above) for guidance.)

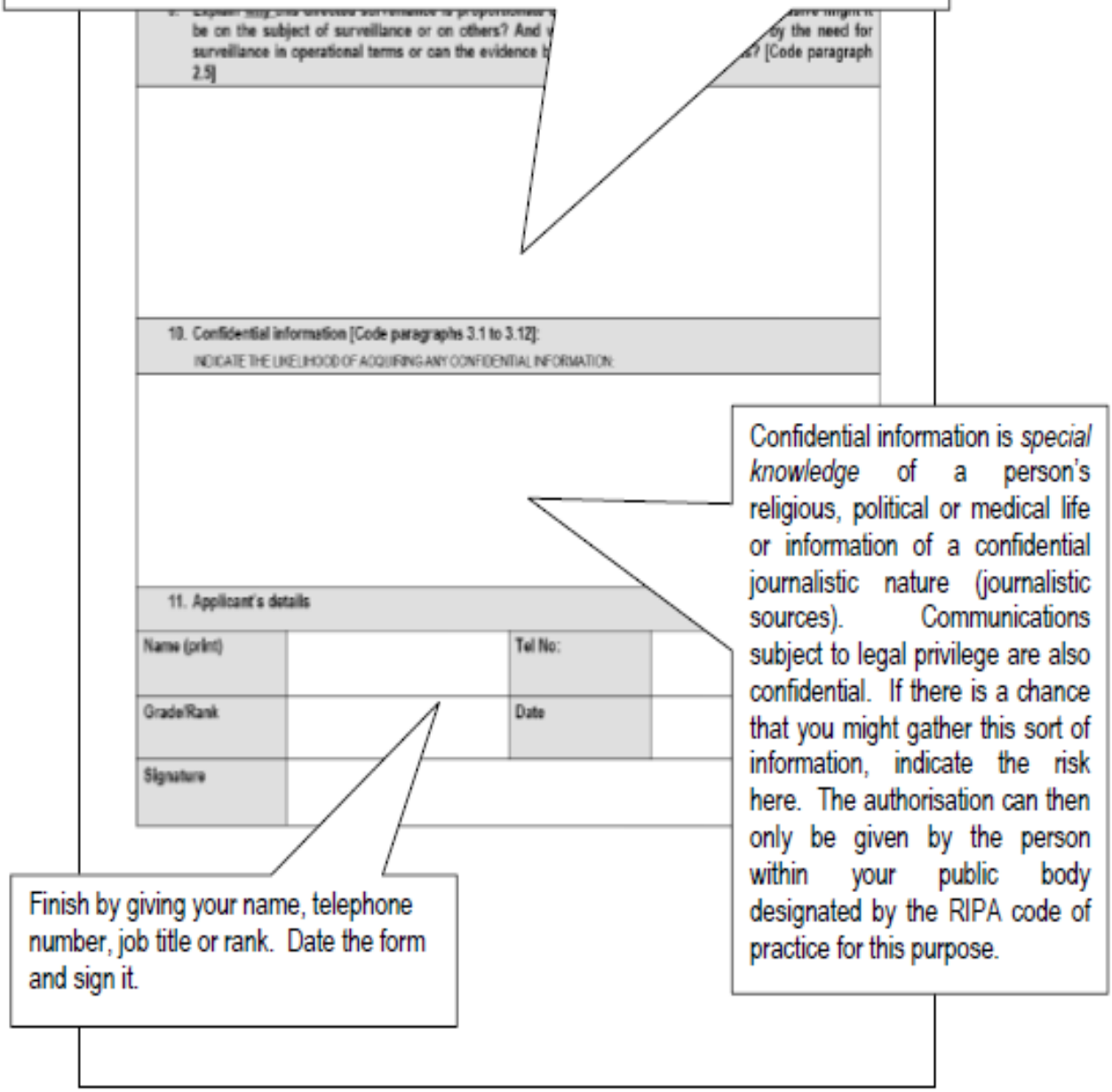
Appendix 10 - The RIPA 1 Form – Guidance on Completion




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?
2. Describe the purpose of the specific operation or investigation.
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.


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

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?



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.