Surrey Heath Borough Council

Surrey Heath House
Knoll Road
Camberley
Surrey GU15 3HD
Telephone: (01276) 707100
Facsimile: (01276) 707177
DX: 32722 Camberley
Web Site: www.surreyheath.gov.uk

Department: Transformation

Division: Democratic Services

Please ask for: Andrew Crawford

Direct Tel: 01276 707139

E-Mail: democratic.services@surreyheath.gov.uk

Tuesday, 17 March 2015

To: The Members of the **Performance and Audit Scrutiny Committee - Audit Meeting** (Councillors: John May (Chairman), David Allen (Vice Chairman), Tim Dodds, Alastair Graham, Beverley Harding, Edward Hawkins, Paul Ilnicki, Lexie Kemp, Chris Pitt, Joanne Potter, Wynne Price, Audrey Roxburgh, Pat Tedder, Alan Whittart and John Winterton)

In accordance with the Substitute Protocol at Part 4 of the Constitution, Members who are unable to attend this meeting should give their apologies and arrange for one of the appointed substitutes, as listed below, to attend. Members should also inform their group leader of the arrangements made.

Substitutes: Councillors Rodney Bates, Glyn Carpenter, Liane Gibson and Ian Sams

Dear Councillor,

A meeting of the **Performance and Audit Scrutiny Committee - Audit Meeting** will be held at Surrey Heath House on **Wednesday, 25 March 2015 at 7.00 pm**. The agenda will be set out as below.

Please note that this meeting will be recorded.

Yours sincerely

Karen Whelan

Chief Executive

AGENDA

Pages

Part 1
(Public)

1 Chairman's Announcements

2 Apologies for Absence

3 Minutes **1 - 2**

To confirm and sign the open minutes of the Audit meeting held on 28 January 2015 (copy attached).

4 Declarations of Interest

Members are invited to declare any Disclosable Pecuniary Interests and non-pecuniary interests they may have with respect to matters which are to be considered at this meeting.

5	**Regulation of Investigatory Powers Act 2000 - Update**	**3 - 64**

Minutes of a Meeting of the Performance and Audit Scrutiny Committee - Audit Meeting held at Surrey Heath House on 28 January 2015

+ Cllr John May (Chairman)
+ Cllr David Allen (Vice Chairman)

+	Cllr Tim Dodds	-	Cllr Joanne Potter
+	Cllr Alastair Graham	+	Cllr Wynne Price
+	Cllr Beverley Harding	+	Cllr Audrey Roxburgh
-	Cllr Edward Hawkins	+	Cllr Pat Tedder
+	Cllr Paul Ilnicki	-	Cllr Alan Whittart
-	Cllr Lexie Kemp	+	Cllr John Winterton
-	Cllr Chris Pitt		

+ Present
- Apologies for absence presented

Substitutes:

Councillor Ian Sams, substituting for Councillor Lexie Kemp.
Councillor Rodney Bates, substituting for Councillor Alan Whittart.

In Attendance: Andrew Crawford, Sarah Groom, Karen Limmer, Kelvin Menon and Alex Middleton.

37/P Chairman's Announcements

The Chairman welcomed Members to the meeting and reminded them that the previous audit minutes, from 23 July 2014 had been held till this, the first subsequent Audit meeting.

38/P Minutes

The minutes of the Audit meeting of the Committee, held on 23 July 2014, were agreed and signed by the Chairman.

39/P 2015/16 Annual Plan for the Internal Audit Service

The Senior Auditor, Alex Middleton, presented a report proposing work programme to cover the municipal year 2015/16. The plan, based on the 3 year medium term Strategic Audit Plan, agreed at a previous meeting, allocated 522 days of work, utilising 2 full time auditors, 80 days of which would be allocated to work required by the Council's external auditors, KPMG.

A number of more critical areas were audited each year, with others being covered on a rolling programme and a contingency kept for issues that arise outside the elements of the Plan.

Progress against the plan and performance of the Audit Team were monitored in the course of the year and any major changes would be discussed and agreed in advance by the Executive Head of Finance and/or the Committee Chairman. Any significant risks or issues identified would be reported to the Committee and senior management, plus the Corporate Risk Management Group.

The Senior Auditor, in response to Member queries, confirmed that the number of days allocated was based on the risk and complexity, but also on the experience of the auditors in those areas, an example being Treasury Management which, whilst being examined yearly had a substantial level of assurance and required less days as a result.

In the previous year, between 15 and 20 audit reports had been issued with 60 to 70 recommendation issued in medium or high risk areas. Of these, only 3 recommendations had yet to be fully implemented and it was anticipated that this would be achieved before a report was submitted to the next meeting of this Committee.

Resolved, that the Annual Audit Plan for 2015/16 be noted and agreed.

Chairman

Regulation of Investigatory Powers Act 2000 – Annual Report on Authorisations

Portfolio:	N/A
Ward(s) Affected:	n/a

Purpose

To report on the number of authorisations made by officers in the municipal year 2014/15

Background

1. Under its terms of reference the Performance and Audit Scrutiny Committee receives an annual report from the RIPA Monitoring Officer in respect of authorisations granted for directed surveillance or the use of covert human intelligence sources to officers pursuant to the powers granted to the Council under the Regulation of Investigatory Powers Act 2000 ("RIPA").

2. The Council's current RIPA Policy provides that any authorisations, including authorisations for renewal, are required to be notified to the Regulation of Investigatory Powers Act Monitoring Officer (RMO).

Current Position

3. As required annually, the RIPA Policy has been reviewed and remains compliant with Home Office guidance. A copy of the current Policy is attached for information.

4. The Office of Surveillance Commission ("OSC") inspected the Council's records of its use of RIPA in November 2014 as part of its 3 yearly inspections of local authorities. During that inspection the OSC made several comments about the current Policy. These were to add further details about the process of obtaining Magistrates approval. The Policy has been altered to reflect this and is published on the Council's website.

5. I am pleased to report that the Inspector, in his conclusion, said;

   This may be regarded as a very satisfactory inspection. A very professional, efficient, knowledgeable and enthusiastic team of officers is extremely very well placed to run a RIPA compliant operation should the Council decide to make use of the RIPA provisions.

Authorisations

6. During the municipal year 2014/2015 there were no authorisations, reviews or renewals under RIPA for the carrying out of direct surveillance.

Recommendation

7. The Committee is advised to note that there was no authorisations for directed surveillance granted during the 2014/15 municipal years.

Background Papers: None

Author: Jessica Harris-Hooton 01276 707314
e-mail: Jessica.harris-hooton@surreyheath.gov.uk

Head of Service: Karen Limmer 01276 707304
e-mail: Karen.limmer@surreyheath.gov.uk
Head of Legal Services

Regulation of Investigatory Powers Act 2000

Use of Covert Directed Surveillance

Use of Covert Human Intelligence Sources

Accessing Communications Data

Policy and Procedure

January 2015

INDEX

	Page No.
Introduction	**3**
Types of Surveillance	**5**
Conduct and Use of Covert Human Intelligence Sources (CHIS)	**9**
The Internet and RIPA	**12**
Authorisation Procedures for Directed Surveillance and CHIS	**13**
Accessing Communications Data	**21**
Authorisation Procedures for Accessing Communications Data	**24**
Working with / through Other Agencies	**27**
The 'Policing' of RIPA	**28**
Consequences of Non-compliance	**29**
Complaints	**30**
Non-RIPA Surveillance	**31**
Oversight by Members	**32**
Appendix One List of Authorising Officers / Authorised Applicants	**33**
Appendix Two RIPA Flow Chart for Directed Surveillance and CHIS	**35**
Appendix Three RIPA Forms, Codes of Practice and Advice	**36**
Appendix Four Notes for Guidance for Authorisations	**37**
Appendix Five Checklist – Can the Council Use RIPA	**40**
Appendix Six The Role of the RIPA Monitoring Officer	**42**
Appendix Seven The RIPA1 Form – Guidance Notes on Completion	**44**
Appendix Eight General Best Practice Advice	**48**
Appendix Nine Extract from the Consolidating Orders	**49**
Appendix Ten Glossary	**50**
Appendix Eleven Judicial Authority	**53**

INTRODUCTION

1. The Regulation of Investigatory Powers Act 2000 ("the Act") came into force on 25 September 2000. The Act regulates the use of powers connected with the *interception of 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 our domestic law. It is unlawful for a public authority to act against a Convention right.

2. This policy and procedures document ("the Policy") sets out the means of compliance with, and use of, the Act by Surrey Heath Borough Council ("the Council") 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. This version of the Policy and Guidance has been updated to take account of the changes in the Protection of Freedoms Act 2012 and SI2012/1500

3. The Council has numerous statutory powers and duties to investigate activities of private individuals, groups and organisations within its jurisdiction for the benefit and protection of the public (collectively known as the Council's "Core Functions"). Such investigations may require the use of DS, CHIS and / or ICD. (There are many reasons why the Council might need to investigate, such as audit investigation, benefit fraud, health & safety compliance, environmental health and pollution control, planning enforcement, control of building works and investigation of its own employees for the purposes of disciplinary proceedings ; this list is not intended to be exhaustive. Some of these areas are Core Functions and, as such, covered by RIPA; others are not and will, therefore, not fall within the RIPA framework.)

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

5. The Council's stated objective is compliance with the provisions of the Human Rights Act 1998, and in particular the provisions of Article 8 obliging respect for an individual's privacy. However, this is a qualified right, not an absolute one, and all investigations involve a legitimate breach of this privacy to a greater or lesser extent ; there are many circumstances where the Council will have a legitimate reason to use ICD, DS or a CHIS as part of the investigation. The Council will always use the Act to authorise these activities, so long as the investigation is a Core Function.

6. RIPA is not available to use for investigations that do not form part of the Council's Core Functions, but this does not preclude the Council's investigators from using DS or CHIS. 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”.

7. **No regulated activity must take place until Judicial Approval has been obtained.** The procedure for Judicial Approval is explained in Appendix Eleven. Before undertaking surveillance and applying for Judicial Approval , the Council must be satisfied that it is undertaken either in connection with a Core Function or with a function that any ordinary employer might have (an “Ordinary Function”), such as the investigation of false claims for sick pay. As all surveillance is likely to intrude upon someone’s human rights (for example, the right to respect for privacy and family life, home and correspondence), 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 documented and the correct authorisations gained, in order that the Council may be accountable for their actions.

8. The Authority hereby appoints all investigation officers and managers to make applications under this part (in accordance with s. 223(1) of the Local Government Act 1972), subject to their inclusion in the approved list by the *RMO*. The Authority authorises the *RMO* to appoint as many investigation officers and managers to make applications under this part as she sees fit. Those officers must be listed at appendix 1(a) and any additions to or deletions from that list must be notified to members as part of the regular reporting protocols.

9. 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 Council’s Head of Legal Services for advice and assistance.

10. The Council 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 the Council’s policy. Furthermore, Officers shall receive appropriate training 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** he has been certified by the Head of Legal Services to do so.

11. The Solicitor shall act as the “*RIPA Monitoring Officer (RMO)*” for all applications, the Principal Solicitor shall act as the Gatekeeper”, the Council’s Head of Legal Services shall discharge the duties of the “*Senior Responsible Officer (SRO)*”, the Council’s Chief Executive or in their absence, the person acting as Head of Paid Service, shall act as the “*Senior Authorising Officer (SAO)”.* Juvenile Sources, Vulnerable Individuals and where knowledge of confidential information is likely to be acquired must be authorised by the SAO.

12. 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. Where

Authorising Officers have suggestions for continuous improvement of this Policy these must be brought to the attention of the Head of Legal Services.

13. **Failure to follow these provisions of this Policy (for example: carrying out surveillance without following the requirements of this Policy) is a breach of the Council's rules, policies and procedures and could be deemed as gross misconduct potentially leading to dismissal.**

TYPES OF SURVEILLANCE

1. 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 overt or covert.

2. **Overt Surveillance**

   Most of the surveillance carried out by the Council will be done overtly – there will be nothing covert about it. In many cases, Officers will be behaving in the same way as a normal member of the public or will be going about Council business openly (such as conducting a site visit for planning enforcement purposes)

   Similarly, surveillance will be overt if the subject has been told that it will happen (for example, where a licensee has been made aware that officers may conduct visits without notice to check that conditions applied to a licence issued under the Licensing Act 2003 are being complied with)

The following are NOT normally Directed Surveillance :

- Activity that is observed as part of normal duties, e.g. by an officer in the course of day-to-day work.
- CCTV cameras (unless they have been directed at the request of investigators) – these are overt or incidental surveillance, and are regulated by the Data Protection Act.
- Targeting a "*Hot spot*", e.g. licensing officers standing on a street to monitor private hire cars plying for hire illegally where this is not part of a planned operation, or surveillance on fly tipping and dog fouling clear up. (Home Office Guidance refers.)
- Test purchases for sale of alcohol to under 18s.

3. **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; it is possible to be covert in Council uniform where, for example, the person is intended to mistake the reason for the officer being there.

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

4. Directed Surveillance

Directed surveillance is surveillance which ~

⇒ is covert; and
⇒ is not intrusive surveillance
⇒ is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable; 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 an investigation)

Private Information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him and others that he comes into contact, or associates, with.

Expectations of Privacy :

Two people are holding a conversation on the street and, even though they are talking together in public, they do not expect their conversation to be overheard and recorded by anyone. They have a 'reasonable expectation of privacy' about the contents of that conversation, even though they are talking in the street. The contents of such a conversation should be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation and otherwise than by way of an immediate response to events.

A Surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

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 some cases overtly) obtained for 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 :

Officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. If the officers chanced to see illegal activities taking place, these could be recorded and acted upon as 'an immediate response to events'.

If, however, the officers intended to carry out the exercise at a specific time of day, when they expected to see unlawful activity, this would not be reconnaissance but directed surveillance, and an authorisation should be considered.

Similarly, if the officers wished to conduct a similar exercise several times, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person or persons and a directed surveillance authorisation should be considered.

5. **Intrusive Surveillance**

RIPA does not authorise local authorities to carry out intrusive surveillance. Intrusive surveillance occurs when the surveillance is

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

Council Officers must NOT carry out intrusive surveillance

Notes about 'Intrusive' :
Surveillance is generally 'Intrusive' only if the person is on the same premises or in the same vehicle as the subject(s) of the surveillance. Carrying out surveillance using private residential premises (with the consent of the occupier) as a 'Static Observation Point' does not make that surveillance 'Intrusive'.

A device used to enhance your external view of property is almost never an *intrusive* device. A device would only become *intrusive* where it provided a high quality of information from inside the *private residential premises*.

If premises under surveillance are known to be used for legally privileged communications, that surveillance must also be treated as *intrusive.*

Examples :
Officers intend to use an empty office to carry out surveillance on a person who lives opposite. As the office is on the 4th floor, they wish to use a long lens and binoculars so that they can correctly identify and then photograph their intended subject covertly. This is NOT *intrusive surveillance*, as the devices do not provide high quality evidence from inside the subject's premises.

Officers intend using a surveillance van parked across the street from the subject's house. They could see and identify the subject without binoculars but have realised that, if they use a 500mm lens, as the subject has no net curtains or blinds, they should be able to see documents he is reading. This IS *intrusive surveillance*, as the evidence gathered is of a high quality, from inside the premises, and is as good as could be provided by an officer or a device being on the premises.

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 are PRP
- Hotel rooms are PRP
- Lorry cabs and camper vans are PRP
- Communal areas (like stairs in a block of flats) are not PRP **but**
- A stairwell in a block of flats, known to be used by a homeless person as their temporary residence **is** PRP
- Canteens and dining areas are not PRP
- Front gardens are not PRP
- Setting up a local authority house for a covert operation (and, therefore) for non-residential purposes is not PRP.

Examples of different types of surveillance

Type of Surveillance	**Examples**
Overt	Civil Enforcement 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

	Enforcement Officer conducting a site visit, 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	Planting a listening or other device in a person's home or in their private vehicle

THE COUNCIL CANNOT AUTHORISE THIS ACTIVITY AND FORBIDS ITS OFFICERS FROM CARRYING OUT INTRUSIVE SURVEILLANCE.

CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

1. **Who is a CHIS**

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

RIPA does not apply to circumstances where members of the public volunteer information to the Council or to contact numbers set up to receive such information (such as a benefit fraud hotline).

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

If a person who provides information voluntarily is asked to obtain further information, it is likely that they would either become a CHIS or that DS authorisation should be considered.

Examples of a CHIS may include:

- Licensing Officers, working with the Police, covertly building a business relationship with a cab company which is believed to be using unlicensed drivers.
- Whistleblowing, when you actively "recruit" an employee to gather information on another employee who is the subject of a criminal investigation, provided this is undertaken within a formal framework (refer to the Council's Raising Concerns at Work (Whistleblowing) Policy).
- Food Safety Officers posing as customers to get information on what is being sold at premises and developing a relationship with the shopkeeper beyond that of supplier and customer.

2. **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 and the decision to use a CHIS in the first place.

3. **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.

By contrast, 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 in the form of covert directed surveillance. 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 in this manner should be considered as a CHIS.

4. **Use of juveniles as CHIS**

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

Authorisations for juvenile CHIS must not be granted unless: -

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

⇒ The risk assessment has been considered by the Authorising Officer and he is satisfied that any risks identified in it have been properly explained; and

⇒ The Authorising Officer has given particular consideration as to whether the child is to be asked to get information from a relative, guardian or any other person who has for the time being taken responsibility for the welfare of the child.

N.B.: A child under the age of 16 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 there will at all times be a person who has responsibility for ensuring that an appropriate adult will be present between any meetings between Council representatives and a CHIS under 16 years of age.

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

5. **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.

Any vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances.

Authorisations for the use of a vulnerable individual as a CHIS can only be granted by the SAO as Head of Paid Service or, in her absence, the person acting as Head of the Paid Service.

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

THE INTERNET AND RIPA

Nowadays investigators make much use of the internet in the course of their enquiries. Many of these enquiries are simple 'open source' enquiries and are unlikely to amount to either Directed Surveillance or the use of a Covert Human Intelligence Source. There are, however, circumstances under which RIPA authorisation may be appropriate.

1. Normal usage

Where an investigator makes normal background checks on the internet, accessing pages that are in the public domain on a single occasion, this would be considered normal usage. Under these circumstances, whilst full records must obviously be kept (in order to comply with the Criminal Procedure and Investigations Act) there is no need for investigators to seek authorisation to make these enquiries. During the course of the investigation, it would be normal for an investigator to make very occasional checks on pages, in order to confirm the information contained therein or, for example, to check for changes just prior to interview.

If, on the other hand, investigators wish to make regular checks on pages, in order to keep check on a suspect's activities, this may amount to Directed Surveillance.

2. Directed Surveillance

Where investigators make regular checks of a page, in order to monitor activity, this may amount to Directed Surveillance. This is because the person, whilst posting to a public forum, site or page, may well not expect the Local Authority to be watching them.

An analogy must be drawn between the electronic world and the 'real' world – if investigators were to go to a public house, in order to listen to a conversation that the suspect was having, this would amount to Directed Surveillance; visiting an online forum for the same purpose is no different.

You wish to covertly watch a shop, in order to see if the shopkeeper is selling unlawful items. This is Directed Surveillance. That same shopkeeper has an online shop that you wish to check every day. What is the difference?

3. Covert Human Intelligence Source

Looking at publicly available pages is normally considered ‘Open Source’ investigation but the situation changes if investigators are required to request access, in order to view the page.

If investigators have to create or maintain a ‘personal or other relationship’ in order to access information, this probably amounts to becoming a Covert Human Intelligence Source. A good example of this is ‘Facebook’, where a profile may be available for all to view (‘Open Source’ or Directed Surveillance) or may require investigators to send a friend request and have that request accepted.

An exception would be where, for example, the officer uses an identity that is manifestly overt (Surrey Heath Trading Standards) and sends the request from this identity. Under these circumstances, the viewing of the page would amount to monitoring and not Directed Surveillance or becoming a Covert Human Intelligence Source.

Officers are instructed to use the procedures outlined in this policy (either RIPA or Non-RIPA), if the above circumstances apply.

AUTHORISATION PROCEDURES FOR DIRECTED SURVEILLANCE AND CHIS

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

2. **Authorising Officers**

DS and CHIS can only be authorised by Authorising Officers or the SAO who are named in this policy; the list of Authorising Officers appears at Appendix One. Authorising Officers will be removed from the list if they do not attend the required training programmes. 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.

Authorisations under RIPA are separate from, and in addition to, any delegated authority that may be required to act under the Council'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.

Only the SAO can authorise the use of a CHIS who is a juvenile or vulnerable person or in the case of confide

3. **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 (Central Record) of all those individuals who have undergone such training.

4. **Application Forms**

(a) 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.

(b) A Gatekeeper role is conducted by Julia Hutley-Savage, Principal Solicitor, who, if requested to do so by an applicant for an Authorisation, will check the quality of applications before these are submitted to an Authorising Officer and advise whether the application demonstrates sufficient grounds for authorisation.

(c) The RMO role is conducted by Jessica Harris-Hooton, Council Solicitor, and the extent this role is explained in Appendix Six.

5. **Grounds for Authorisation**

Local Authorities can only authorise the use of directed surveillance under RIPA for the purpose of detecting crime or preventing disorder if this involves a criminal offence(s) 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 offences relating to the latter are in article 7A of the 2010 Order. The link can be found at Appendix Three.

Recent guidance from the Home Office has confirmed that this limitation to the circumstances where directed surveillance can be undertaken or a CHIS used does not cover the investigation of circumstances which may lead to the issue of a statutory notice (for example, an enforcement notice or an abatement notice). The Home Office has expressed the view that prior to the issue of a statutory notice only overt surveillance may be undertaken.

6. Assessing the Application Form

Before an Authorising Officer signs a Form he must:

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

(b) satisfy himself that the RIPA authorisation is:
- ⇒ **in accordance with the law ;**
- ⇒ **necessary** in the circumstances of the particular case on the ground available to the Council ;
- ⇒ **proportionate** to what it seeks to achieve ; and
- ⇒ the **criminal offence** being investigated is punishable by a maximum term of imprisonments of **at least 6 months**;

(c) 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;

(d) 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 of minimise (so far as is possible) collateral intrusion and this may be relevant to the issue of proportionality;

(e) set a date for the review of the authorisation;

(f) allocate a Unique Reference Number for the application as follows:

Year / Division / Number of Application; and

(g) Ensure that a copy of the RIPA form is forwarded to the RMO for entry onto the Central Record **within 48 hours of the relevant authorisation being given**.

NB: **The application MUST make it clear how the proposed intrusion is necessary and how an absence of this evidence would have a prejudicial effect on the outcome of the investigation. If it does not, the application MUST be refused.**

Showing 'Necessity'

The application should identify the specific offence being investigated (including section and act) and the specific point(s) to prove that 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.

7. **Additional Safeguards when authorising a CHIS**

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

(a) be satisfied that the **conduct** and / or the **use** of the CHIS is proportionate to what is sought to be achieved;

(b) be satisfied that **appropriate arrangements** exist for the management and oversight of the CHIS; this includes health and safety issues;

(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

(e) ensure **records** contain particulars and are not available except to those persons who have a need to know.

8. **Duration**

The RIPA authorisation must be reviewed in accordance with the time stated 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 a 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, 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 the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into accounts 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

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 them.

- 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.

9. Confidential Information

The Act does not provide any special protection for "confidential information", but there are slight differences in the process. However, 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 material is anything which is:

⇒ 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.

NOTE: Directed surveillance is treated for the purposes of RIPA as intrusive surveillance, where the surveillance takes place in locations where it is known that legal consultations are taking place. 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 concerning an individual (whether living or dead) who can be identified from it.

Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

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 Material

Confidential Journalistic Material 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.

10. **Additional Safeguards for Confidential Information**

Directed Surveillance
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
⇒ Whether the purpose (or one of the purposes) of the use of surveillance or a CHIS is to obtain such confidential information

Additional safeguards are also to be imposed in that: -

⇒ The Authorising Officer must be the SAO or, in her 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 to be disclosed to those who have a clear and substantial need to know and for a specific and proper purpose. (Handling Code 4 or 5).
⇒ Confidential material must be clearly marked as such and accompanied by a clear warning of its confidentiality (Handling Code 4 or 5).

N.B.: If you have any doubt about the handling and dissemination of confidential information, seek advice from a legal adviser within the Council *before* any further dissemination of the material takes place.

Where an Authorising Officer does authorise 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.

11. **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 surveillance, it is monitoring. (Officers must, however, be aware of the risk to health and safety of the person allowing you to use 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, provided the guidance in this section has been followed.

Devices that record sound could be subject to suggestions that they are surveillance devices. This Council is clear that this is not the case, as the subject has been clearly informed that their noise levels will be monitored. Furthermore, the device is only recording noise that is clearly audible outside the monitored premises (such as in a neighbour's house or from the public highway).

Devices that record sound must be set so as to only record noise at the levels that are normally audible to the human ear at the location in which the device is located.

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 intrusive surveillance.

Officers are expressly forbidden from setting up devices EXCEPT as set out in this section.

In the event that Officers wish to carry out surveillance 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 Council to act in this way.

Surveillance equipment will only be installed in residential premises if a member of the public has requested help or referred a complaint to the

Council. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant.

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 but only information about the location of that particular device at any one time. However, the subsequent use of that information coupled with other surveillance activity which may obtain private information, could interfere with Article 8 rights.

Examples of Where Covert Surveillance Equipment Might be Used

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.

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.
A person is suspected of mis-selling service to persons on the street. Officers gain authorisation to approach the man and record the conversation, using a concealed tape recorder.

Any request by a Council Officer to a resident to keep a video / audio / written diary as part of a Covert evidence-gathering exercise will be regarded as a Covert Surveillance exercise conducted on behalf of the Council and must be authorised appropriately.

Generally, information gained under this type of operation will be given a dissemination code of 4 or 5, that is access will generally only be allowed to limited and prescribed parties, including law enforcement agencies, and prosecution agencies, and would have special condition 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 conduct of a source, whether used or unused material, must be recorded and retained and revealed to the prosecutor according to the Criminal Procedure and Investigations Act (CPIA).

12. **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.**

ACCESSING COMMUNICATIONS DATA

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

2. **Communications Data**

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

In essence, the Council 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.

3. The Council 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

4. **Accessing Communications Data**

The Act provides two different ways of authorising access to communications data: through an authorisation under section 22(3) and by a notice under section 22(4). An authorisation would allow the Council 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 Council. A designated person decides whether or not an authorisation should be granted or a notice given. For practical reasons, generally the Council will only be using the Notice route to access communications data.

<u>Applicant</u>

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 public 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 22(2) of the Act; for local authorities this 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, both 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).

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 this Act.

Single Point of Contact

The single point of contact (SPoC) is either an accredited individual or a group of accredited individuals trained to facilitate 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 the role of a SPoC.

An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides 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 the 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;
- ⇒ provide assurance to CSPs that authorisations and notices are authentic and lawful;
- ⇒ assess any cost and resource implications to both the public authority and the CSP of data requirements.

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

The SPoC may be an individual who is also a designated person.

AUTHORISATION PROCEDURES FOR ACCESSING COMMUNICATIONS DATA

1. Accessing communications data can only be lawfully carried out if properly authorised and if it is carried out in strict accordance with that authorisation. Generally the Council will only be using the Notice route to access communications data.

2. **Designated Persons**

Approval for the accessing of communications data can only be given by a 'designated person' who holds a certificate from the Head of Legal Services. This is not to be confused with those officers authorising covert directed surveillance. A list of Designated Persons within the Council 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 delegated authority that may be required to act under the Council'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.

3. **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 the Central Record of all those individuals who have undergone such training.

4. **Application Forms**

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

5. **Grounds for Application**

An application for accessing communications data may be granted by a Designated Person where he believes that the authorisation is necessary in the circumstances of the particular case. However, the only statutory ground under which the Council can access communications data is for the purpose of preventing or detecting crime or of preventing disorder.

6. **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 access *traffic data* as defined by section 21(4)(a) of the Act.

7. 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 he must ~

(a) Be mindful of the Council's Policy and Procedures Document, the training provided and any other guidance issued, from time to time, by the Head of Legal Services

(b) Satisfy himself that the RIPA authorisation is ~
- ⇒ **in accordance with the law**
- ⇒ **necessary** in the circumstances of the particular case on the ground available to the Council
- ⇒ **proportionate** to what it seeks to achieve

(c) In assessing whether the accessing of communications data is proportionate, consider whether there are other methods of gathering the information. The least intrusive method will be considered to be the most proportionate method.

8. 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.

9. Single Point of Contact

All Notices should be channelled through the Single Point of Contact (SPoC) as the CSPs will only deal with requests from authorised/accredited SPoCs. The SPoC must have undergone accredited training and can ~

- ⇒ assess whether access to communications data is reasonably practicable for the postal or telecommunications operator

⇒ advise applicants and designated person 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 Council can seek
⇒ provide safeguards for authentication
⇒ assess any cost and resource implications to both the Council 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 Council and the CSP.

10. Urgent Approvals

There is NO provision for the Council to grant urgent approvals for accessing communications data. Applications can only be made in the appropriate manner.

11. 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 Office should specify a shorter period if that is satisfied by 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.

WORKING WITH / THROUGH OTHER AGENCIES

1. When some other agency (for example, Police, HM Revenue and Customs etc) has been instructed on behalf of the Council to undertake any action under RIPA, this Policy and the Forms in it must be used (as per the normal procedure) and the agency must be advised or kept informed, as necessary, of the various requirements. 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).

2. When some other agency wishes to use the Council'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 Council resources, he must obtain a copy of that agency's RIPA form for the record, a copy of which must be passed to the Head of Legal Services in the usual manner) and / or relevant extracts from the form which are sufficient for the purposes of protecting the Council and the use of its resources

3. **If in doubt, you should consult with the Head of Legal Services at the earliest opportunity**

THE "POLICING" OF RIPA

1. RIPA is overseen by Surveillance Commissioners, who have all held high judicial office prior to their appointment. They 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

2. This Council has, in following the general advice from the OSC appointed a SRO (see Appendix 9 part 2), who is responsible for corporate oversight of the RIPA process. The SRO is Karen Limmer, who is the Council's Head of Legal Services

3. 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 Office of the Surveillance Commissioner, may be considered to have committed 'gross misconduct' and be liable to disciplinary proceedings.

4. 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 case challenge or as a defence to a case brought by the Council, or in a referral to the local government Ombudsman, or a complaint to the Information Commissioner, from where compensation awards can flow.

CONSEQUENCES OF NON COMPLIANCE

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

1. **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 at Section 4) are not handled properly, the evidence obtained may be held to be inadmissible. Section 78 of the Police and Criminal Evidence Act 1984 allows for evidence that was gathered in a way that affects the fairness of the criminal proceedings to be excluded. The Common Law Rule of Admissibility means that the court may exclude evidence because its prejudicial effect on the person facing the evidence outweighs any probative value the evidence has (probative v prejudicial).

2. **Legal Challenge –** as a potential breach of Article 8 of the European Convention on Human Rights, which establishes a "right to respect for private and family life, home and correspondence", incorporated into English Law by the Human Rights Act (HRA) 1998. This could not only cause embarrassment to the Council but any person aggrieved by the way a local authority carries out Covert Surveillance, as defined by RIPA, can apply to a Tribunal – see section 15.

3. **Offence of unlawful disclosure –** disclosing personal data as defined by the DPA that has been gathered as part of a surveillance operation is an offence under Section 55 of the Act. Disclosure can be made but only where the officer disclosing is satisfied that it is necessary for the prevention and detection of crime, or apprehension or prosecution of offenders. Disclosure of personal data must be made where any statutory power or court order requires disclosure.

4. **Fine or Imprisonment** – Interception of communications without consent is a criminal offence punishable by fine or up to two years in prison.

5. **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.

6. **Disciplinary Action** – Failure of officers to comply with this Policy and Guidance is a disciplinary offence under the Council's Policies and Procedures.

COMPLAINTS

1. If any person complains about matters covered by this policy, they will be directed to the Council's Complaints Procedure, and invited to use it if they wish to make a complaint regarding breach of this Policy and Guidance. ANY complaint received will be treated as serious and investigated in line with this authority's policy on complaints. **Regardless of this, the detail of an operation, or indeed its existence, must never be admitted to as part of the complaint handling process.** This does not mean it will not be investigated, just that the result of any investigation would be entirely confidential and not disclosed to the complainant.

2. 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.

3. 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. This Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure can be obtained from the following address:

   Investigatory Powers Tribunal
   PO Box 33220
   London
   SW1H 9ZQ

   020 7035 3711.

4. Furthermore, *Judicial Review* is available to any person who believes their rights have been unlawfully breached outside the scope of RIPA authorisation.

NON-RIPA SURVEILLANCE

1. RIPA does not grant any powers to carry out surveillance, it simply provides a framework that allows public authorities to authorise surveillance in a manner that ensures compliance with the European Convention on Human Rights.

2. Equally, RIPA does not prohibit surveillance from being carried out or require that surveillance may only be carried out following a successful RIPA application.

3. Whilst it is the intention of the Council to use RIPA in all circumstances where it is available, for a local authority, this is limited to preventing or detecting crime or disorder. The Council recognises that there are times when it will be necessary to carry out covert directed surveillance when RIPA is not available to use. This is known as Non-RIPA Surveillance.

Non-RIPA Surveillance

If your investigation is into internal matters that may lead to criminal proceedings, RIPA may be available for you to use, but this is not always the case.

Example

If you are investigating allegations that a member of staff is claiming vehicle mileage when they are actually using public transport, and you are intending to use the evidence you gain for disciplinary purposes only, then RIPA would not be available for you to use. If you intended to take civil proceedings to recover expenses, RIPA would not be available to use. In both cases, any intended surveillance would be Non-RIPA Surveillance

If, however, you intended to prosecute that member of staff for fraud, RIPA may be available for you to use.

4. Under such circumstances, where it is intended to carry out Non RIPA Surveillance, a RIPA application must be completed and clearly endorsed in red 'NON-RIPA SURVEILLANCE' along the top of the first page.

5. The application must be submitted to a RIPA Authorising Officer in the normal fashion, who must consider it for Necessity and Proportionality in the same fashion as they would a RIPA application.

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

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

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

OVERSIGHT BY MEMBERS

1. Elected Members shall have oversight of the Policy and shall review that Policy annually.

2. Elected Members shall receive a report on the use of RIPA regulated activity by officers of the Council every three months.

3. The report to members shall be produced by the RMO and presented to the Elected Members (or to such a sub-committee as the full council shall deem appropriate to constitute 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 product obtained.

4. Alongside this report, the RMO and SRO will report details of 'Non-RIPA' surveillance in precisely the same fashion.

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

6. Elected Members may not interfere in individual authorisations. Their function is to, with reference to the reports; satisfy themselves that the Policy is robust and that it is being followed by all officers involved in this area. Although it is elected members who are accountable to the public for council actions, it is essential that there should be no possibility of political interference in law enforcement operations.

APPENDIX ONE

LIST OF AUTHORISING OFFICERS

POST	NAME
Executive Head of Community	Tim Pashen
Executive Head Regulatory	Jenny Rickard
Investigations Manager	Julia Greenfield

LIST OF DESIGNATED PERSONS FOR APPROVING THE ISSUE OF A NOTICE IN RESPECT OF ACCESS TO COMMUNICATIONS DATA

POST	NAME
Chief Executive	Karen Whelan
Head of Legal Services	Karen Limmer

SINGLE POINT OF CONTACT FOR ACCESSING COMMUNICATIONS DATA (SPoC)

POST	NAME
SPoC	
Investigations Manager	Julia Greenfield
Gatekeeper	
Principal Solicitor	Julia Hutley-Savage

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 certified by the Head of Legal Services to do so and are NAMED in the list.

B. Only the Chief Executive or, in her absence, the Head of Legal Services is authorised to sign forms relating to Juvenile Sources, Vulnerable Individuals and where knowledge of confidential information is likely to be acquired.

C. If an Executive Head wishes to add, delete or substitute a post, he must refer such a request to the Head of Legal Services for consideration.

APPENDIX ONE (A)

COUNCIL'S AUTHORISED APPLICANTS

In order for the Authority's RIPA authorisations to take effect, they must be approved by a Magistrate. That process requires applicants in person to appear for the Authority and the official court service guidance makes it clear that these should be investigators not lawyers.

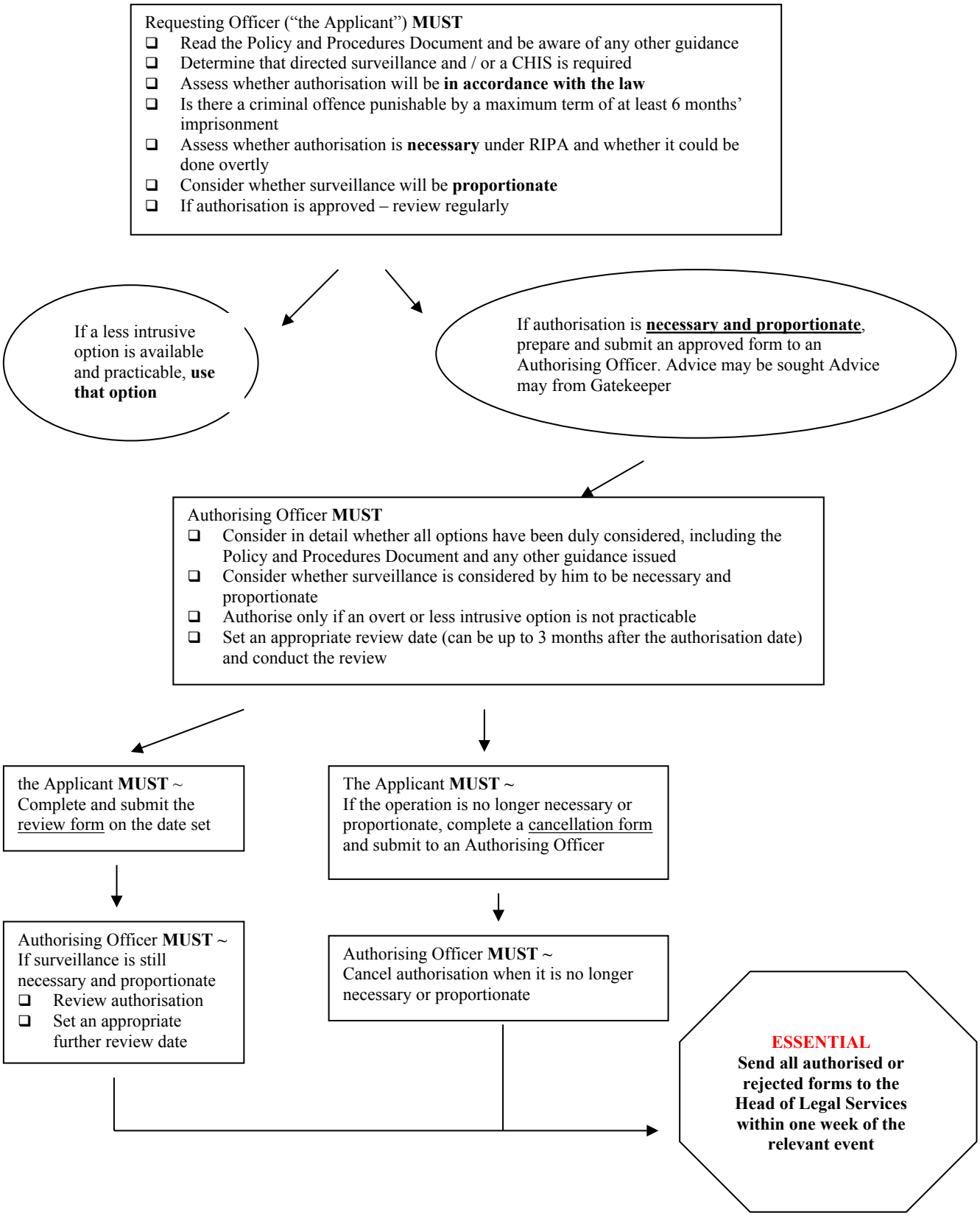
Any person from this Authority wishing to make an application must be named in this annex and must take to court a copy of this annex and their official identification.

I certify that the following have been appointed under section 223(1) of the Local Government Act 1972 to appear for the Authority and are approved applicants in accordance with section 8 of this policy :

Name	Section	Appointed from	Appointment terminated
Julia Greenfield	Audit and Investigations	15/10/14	
Alexandra Gilkes	Audit and Investigations	15/10/14	
Kevin Elkins	Audit and Investigations	15/10/14	

APPENDIX TWO

RIPA FLOW CHART FOR DIRECTED SURVEILLANCE AND CHIS



APPENDIX THREE

RIPA Forms, Codes of Practice and Advice

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

- The most up-to-date RIPA forms must always be used. These are available from the Home Office website and may be found by following this link :

https://www.gov.uk/government/organisations/home-office/series/ripa-forms--2

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

—Covert Surveillance and Property Interference
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-covert

—Covert Human Intelligence Sources
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-human-intel

—Acquisition & Disclosure of Communications Data
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition
Guidance for Local Authorities obtaining judicial approval prior to using covert techniqueshttps://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

- The Act is available here :

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

- The 2010 Order detailing the offences relating to the underage sale of alcohol and tobacco
-

http://www.legislation.gov.uk/uksi/2010/9780111490365/contents

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

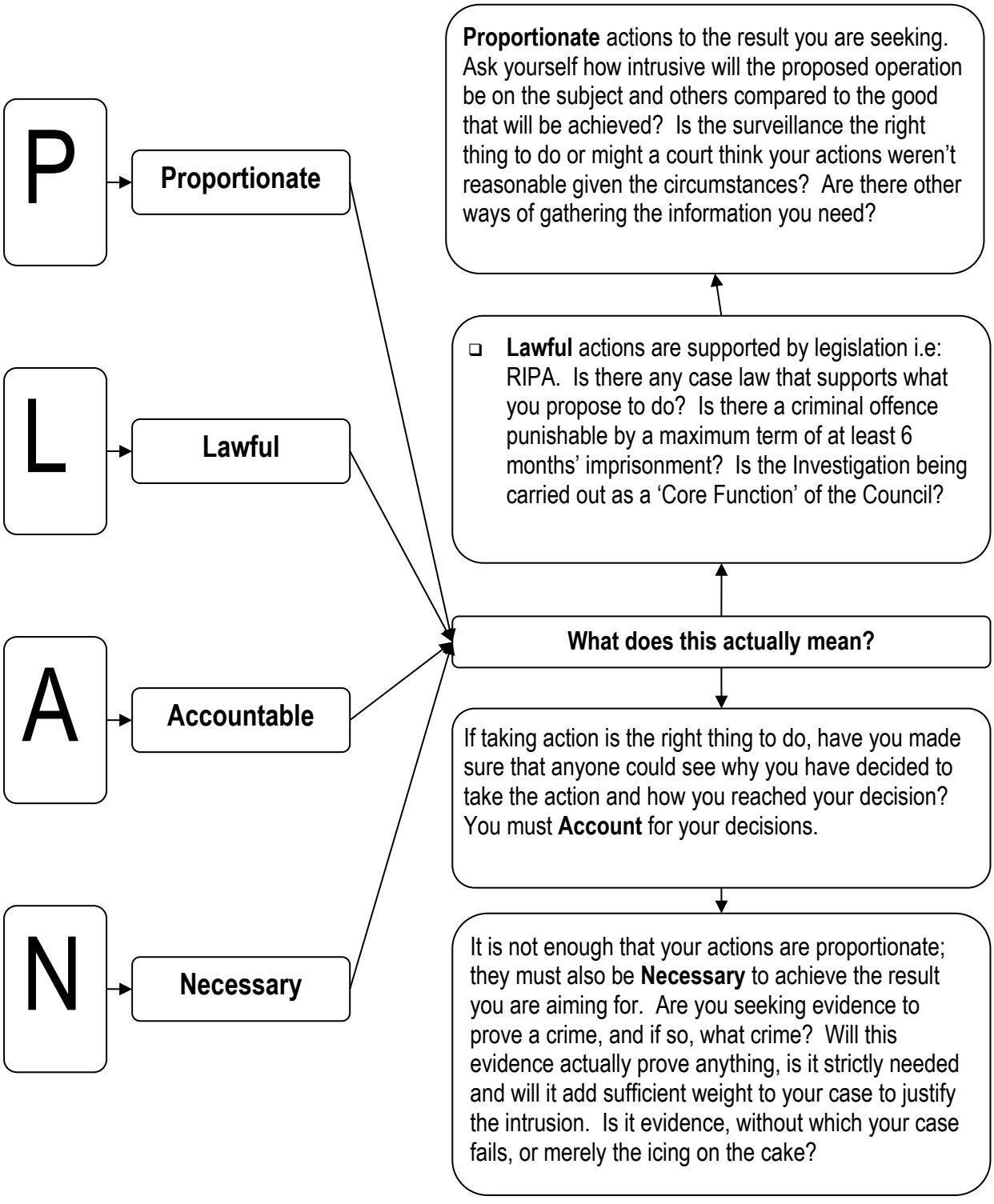
http://surveillancecommissioners.independent.gov.uk/

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

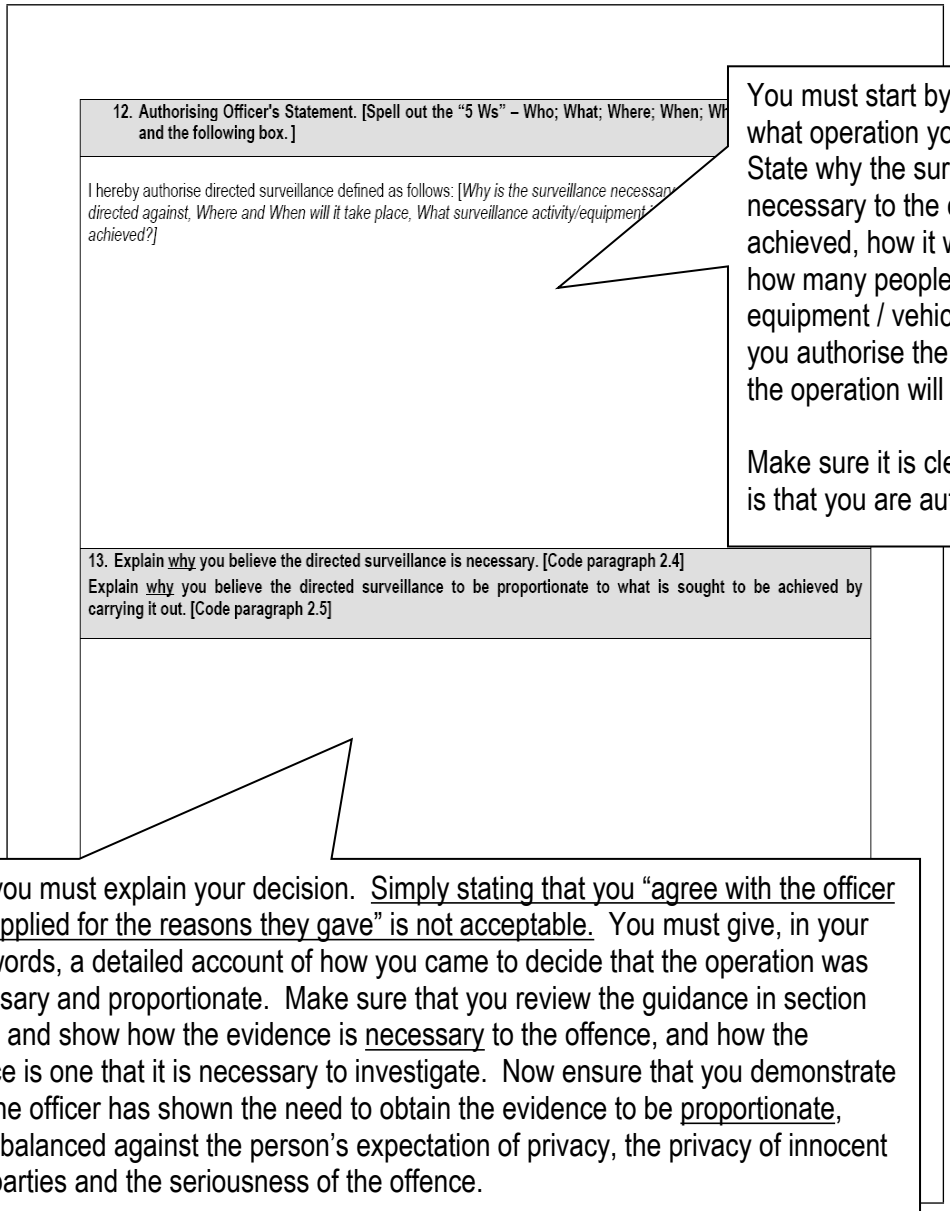
If you have any problems accessing these links, you must report this immediately to the SRO.

APPENDIX FOUR

Notes for Guidance for Authorisation – Directed Surveillance


P
Proportionate
L
Lawful
A
Accountable
N
Necessary
Proportionate actions to the result you are seeking. Ask yourself how intrusive will the proposed operation be on the subject and others compared to the good that will be achieved? Is the surveillance the right thing to do or might a court think your actions weren't reasonable given the circumstances? Are there other ways of gathering the information you need?
Lawful actions are supported by legislation i.e: RIPA. Is there any case law that supports what you propose to do? Is there a criminal offence punishable by a maximum term of at least 6 months' imprisonment? Is the Investigation being carried out as a 'Core Function' of the Council?
What does this actually mean?
If taking action is the right thing to do, have you made sure that anyone could see why you have decided to take the action and how you reached your decision? You must Account for your decisions.
It is not enough that your actions are proportionate; they must also be Necessary to achieve the result you are aiming for. Are you seeking evidence to prove a crime, and if so, what crime? Will this evidence actually prove anything, is it strictly needed and will it add sufficient weight to your case to justify the intrusion. Is it evidence, without which your case fails, or merely the icing on the cake?

Authorising Officer's Statement



12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Wh
and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessar*
directed against, Where and When will it take place, What surveillance activity/equipment
achieved?]

13. Explain why you believe the directed surveillance is necessary. [Code paragraph 2.4]
Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]

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.

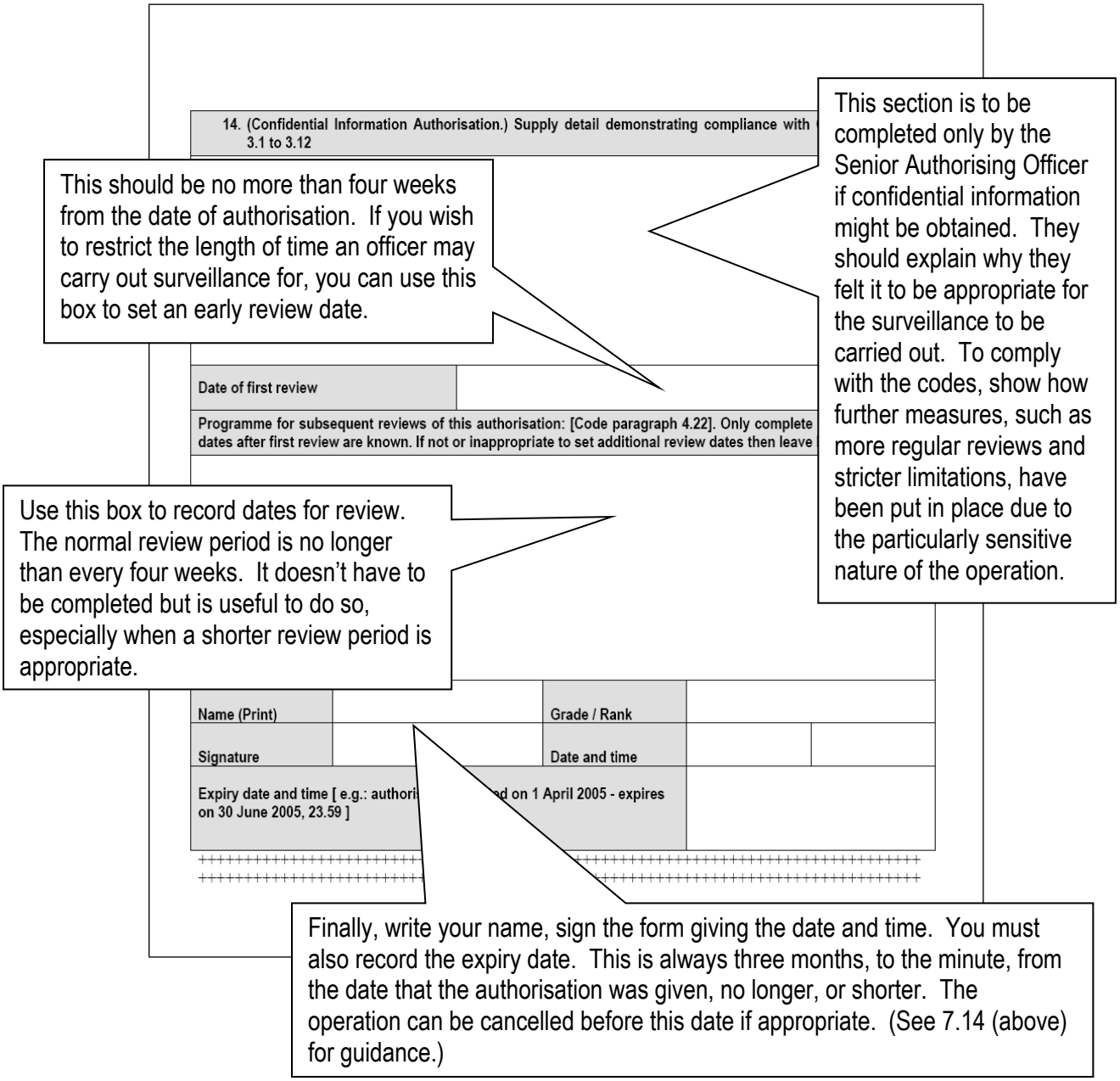
Now you must explain your decision. Simply stating that you "agree with the officer who applied for the reasons they gave" is not acceptable. You must give, in your own words, a detailed account of how you came to decide that the operation was necessary and proportionate. Make sure that you review the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

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

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

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

Authorising Officer's Statement



APPENDIX FIVE

Checklist – Can the Council 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's / 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 in circumstances where it is not reasonably practicable to get authorisation. If the proposed activity has been planned in advance and not just the 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 Council and involves a criminal offence?

In order to use RIPA, the investigation *must* pertain to one of the 'core functions' of the Council – that is a function that you carry out because you are a local authority (such as investigating benefit fraud or looking into allegations of fraudulent subletting). If the investigation is an 'ordinary

function' of the Council (such as allegations of fake sickness or theft from the stationary cupboard, which would lead to internal disciplinary action) RIPA is *not* available to use.
The directed surveillance must be for one of the following reasons:

- To prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** relate to the underage sale of alcohol and tobacco.

- For the purposes of preventing disorder which involves a criminal offence punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment

APPENDIX SIX

The Role of the RIPA Monitoring Officer

The RMO for the Council is the Council's Solicitor.

The RMO 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 authorise.
- Removing people from list if code not followed / training skipped etc.
- Checking for updated advice (OSC website etc.).
- Drawing to Head of Paid Service and Leader of the Council's notice of potential problems.

Each individual authorising officer is personally responsible for reporting the following information to the RMO 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 council's interests.

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

The Authorised Officer should also keep the following. There is no requirement for this to form part of the Central Record maintained by the RMO:

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

Records must be retained in accordance with Data Protection principles.

Storage of Authorisation Forms

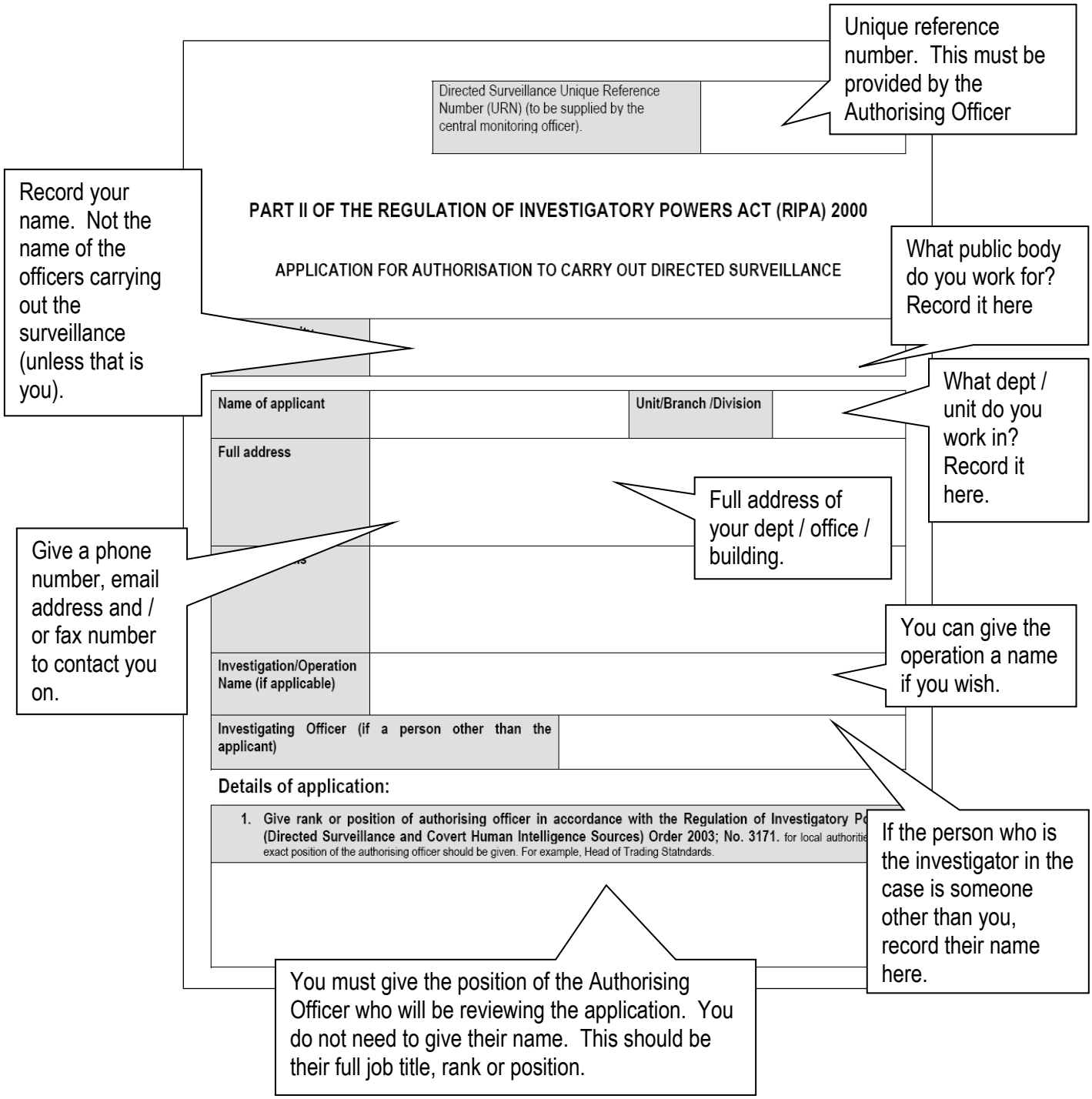
The Policy makes the Chief Executive and each Executive Head of the Council responsible for organising sufficient systems within their service.

The original forms must be retained on the investigation file. Copies must be retained by both the Authorising Officer and the RMO within the Central 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.

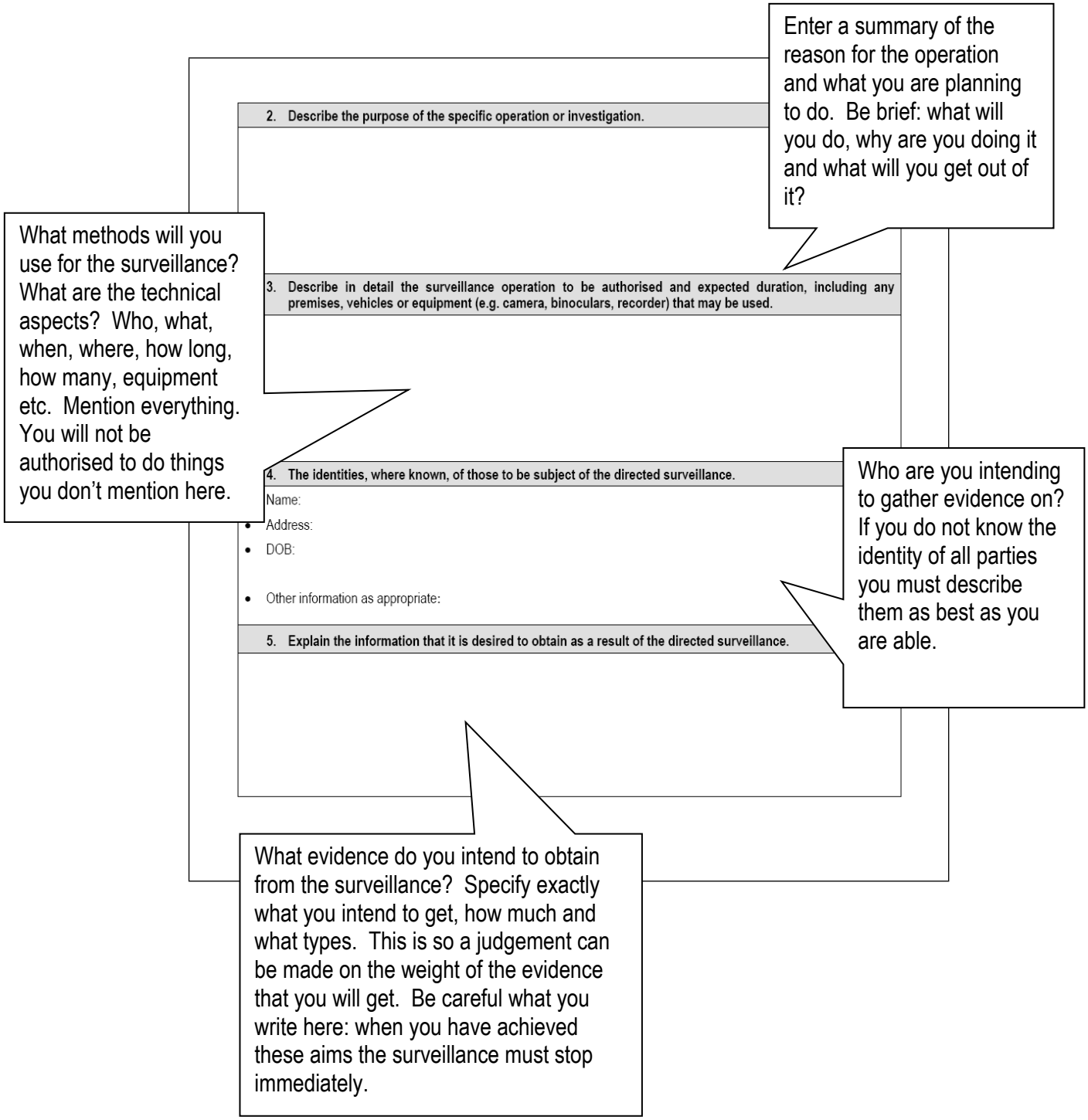
The RMO will retain records for at least three years after the completion of the investigation. All officers are reminded of Data Protection requirements about retention and storage of documents. If in doubt, advice must be sought from the RMO.

APPENDIX SEVEN

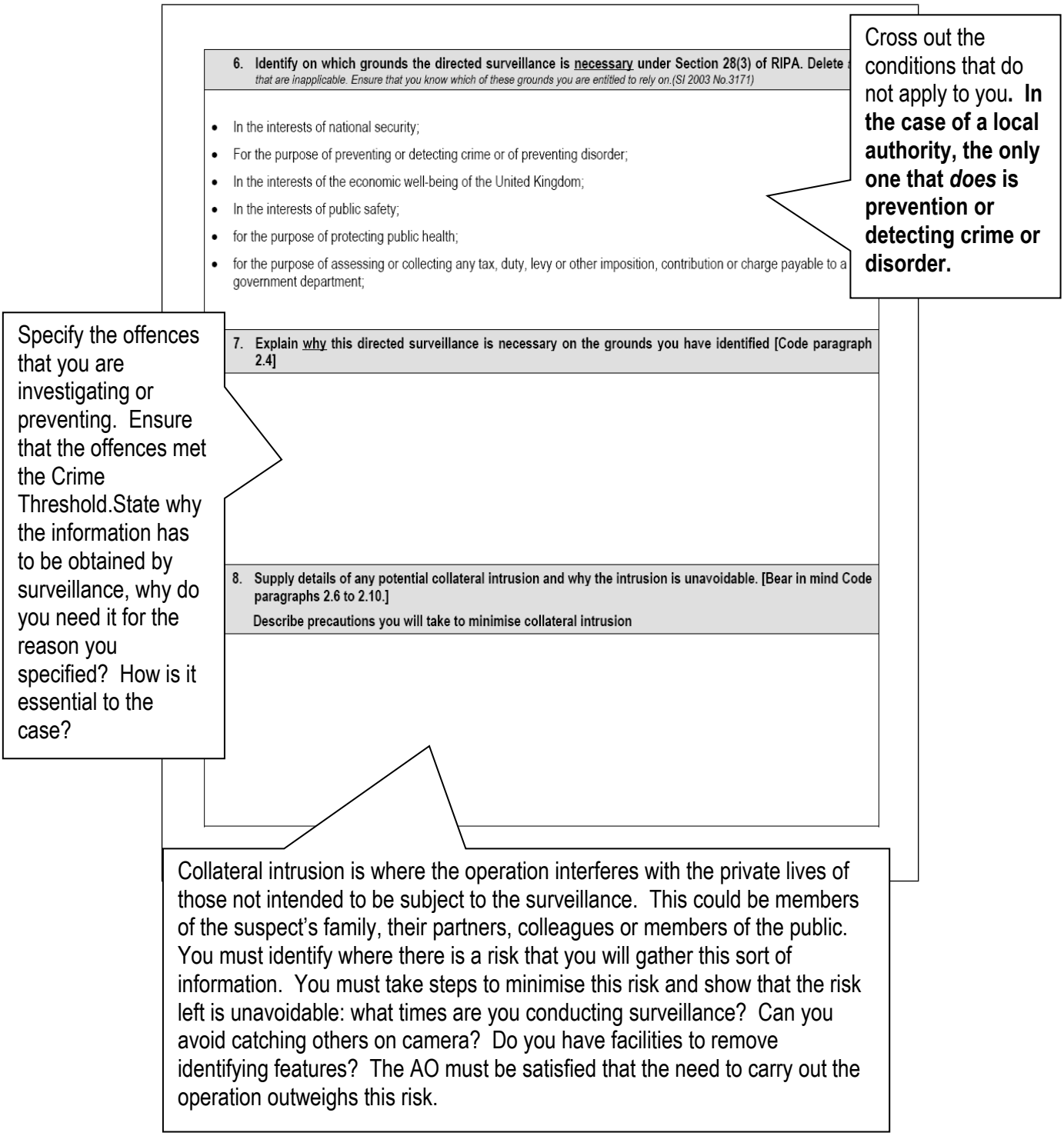
The RIPA 1 Form – Guidance Notes on Completion



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. This is so a judgement can be made on the weight of the evidence that you will get. Be careful what you write here: when you have achieved these aims the surveillance must stop immediately.

Page Three



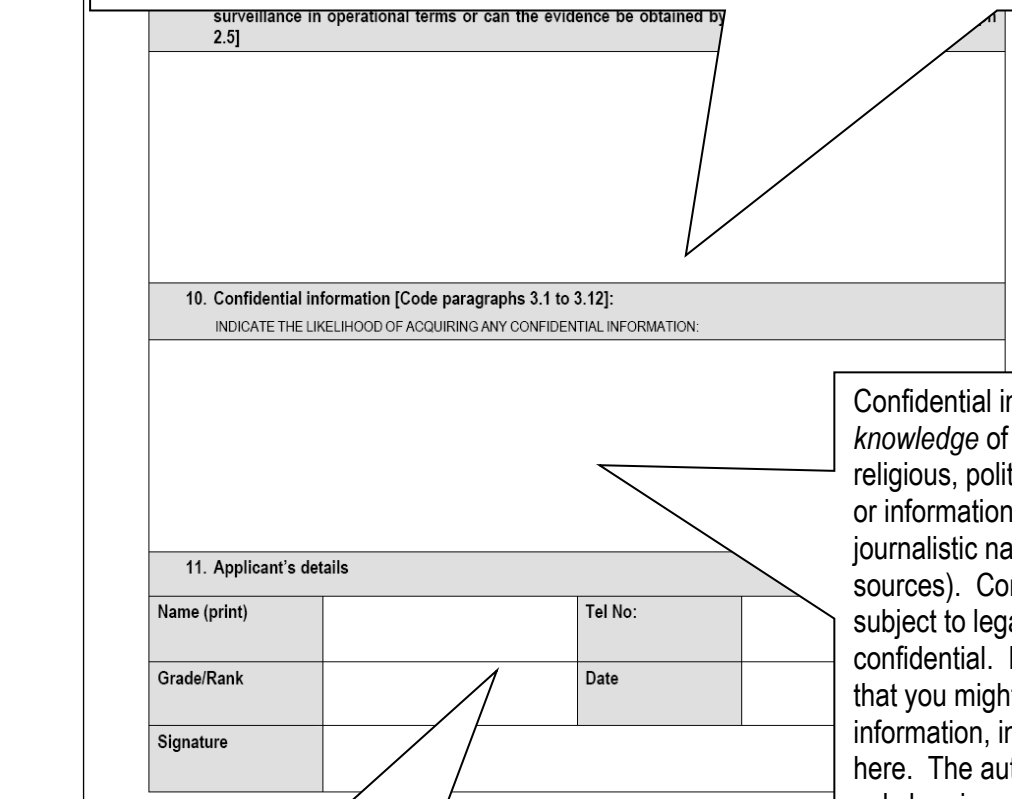
Cross out the conditions that do not apply to you. **In the case of a local authority, the only one that *does* is prevention or detecting crime or disorder.**

Specify the offences that you are investigating or preventing. Ensure that the offences met the Crime Threshold.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'll prejudice the investigation. Tell the AO why the need to carry out the action outweighs the suspect's right to privacy. How serious is the matter? How intrusive will the operation be on the suspect and on others? What might happen if you don't carry out surveillance? Why can't you get the information in other ways? What will be achieved by gathering the evidence?



surveillance in operational terms or can the evidence be obtained by 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.

APPENDIX EIGHT

General Best Practice Advice from the OSC and Code of Practice

1. The following are not statutory requirements or formal provisions of this code, but should be considered as best working practices by all *public authorities* with regard to all *applications* for *authorisations* covered by this code:
    a. a*pplications* should avoid any repetition of information;
    b. information contained in a*pplications* should be limited to that required by the relevant legislation, as laid out in Chapters 5, 6 and 7 of this code;
    c. an *application* should not require the sanction of any person in a *public authority* other than the *authorising officer*;
    d. where it is foreseen that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the *application*;
    e. *authorisations* should not generally be sought for activities already authorised following an application by the same or different *public authority*.

2. Furthermore, it is considered good practice that within every relevant *public authority,* a senior officer should be responsible for:
    a. the integrity of the process in place within the *public authority* to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
    b. compliance with Part II of the 2000 Act, Part III of the 1997 Act and with this code;
    c. engagement with the Commissioners and inspectors when they conduct their inspections, and
    d. where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.
    e. The senior responsible officer should be a person holding the office, rank or position of an *authorising officer* within the relevant public *authority.*

APPENDIX NINE

Extract from the Consolidating Orders

LOCAL AUTHORITIES

353 local authorities in England, 22 in Wales, 32 in Scotland and 26 in Northern Ireland are able to use service use and subscriber data in order to prevent or detect crime or disorder in connection with their statutory functions. Many of these functions are their sole responsibility.

Examples of investigations where covert techniques enable local authorities to trace investigations back to a source individual at a specific address and offer evidence against them in legal proceedings include:

- trading standards (eg action against loan sharks and rogue traders, car fraud, consumer scams, deceptive advertising, counterfeit goods, unsafe toys and electrical goods);
- enforcement of anti-social behaviour orders and legislation relating to unlawful child labour;
- housing/planning (eg intervening to stop and take remedial action against unregulated and unsafe building, breaches of preservation orders, cases of landlord harassment);
- benefits fraud (eg housing benefits, investigating 'living together' and 'working whilst in receipt of benefit' allegations, council tax evasion); and
- environment protection (eg action to stop large-scale waste dumping, the sale of unfit food and illegal 'raves').

The advantages of being able to use communications data to help criminal investigation especially in trade and consumer scams is becoming more important with the growth of the internet and distance selling. Many transactions are now done without buyer and seller coming into contact and the only way of linking offenders to these transactions is by communications data.

A series of media articles last year reported some local authorities' use of covert techniques against activities such as dog fouling and littering. The Government and the Local Council Association have separately made it clear that using RIPA authorisations in these instances would not be a proportionate response. The Home Office is working closely with the Department for Communities and Local Government and the relevant Commissioners to address instances of inappropriate use of covert techniques. The statutory RIPA Codes of Conduct which provide guidance to practitioners are being revised accordingly.

Some media articles have confused what RIPA allows local authorities to do with the more intrusive forms of covert activity conducted by intelligence and law enforcement agencies. Under RIPA local authorities cannot intercept communications *(such as telephone 'tapping' or reading someone's e-mails, texts or post) or enter anyone's house covertly. RIPA limits these covert activities to those public authorities with a national security remit or which are operating against a level of 'serious' crime substantially above that tackled by local authorities.*

WHO? (Authorisation Grade)	WHAT? (Covert Technique)	WHY? (Statutory Purpose)
ENGLAND, WALES, SCOTLAND & N IRELAND Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent	RIPA S21(4) (b) service use (c) subscriber data	RIPA S22(2) (b) preventing or detecting crime or disorder
ENGLAND & WALES Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent The Head of Paid Service or (in his/her absence) a Chief Officer … (Scotland & N Ireland omitted)	RIPA S26(1) (a) directed surveillance (c) conduct & use of CHIS Where Confidential information is likely to be obtained or when a vulnerable person/juvenile is to be used as a CHIS	RIPA S28(3) & S29(3) (b) preventing or detecting crime or disorder

(Consolidating Orders and Codes of Practice, page 43)

APPENDIX TEN

GLOSSARY

Application	a request made to an authorising officer to consider granting (or renewing) an authorisation for directed or intrusive surveillance (under the 2000 Act), or interference with property or wireless telegraphy (under the 1994 or 1997 Act). An application will be made by a member of a relevant public authority.
Authorisation	an application which has received the approval of an authorising officer. Depending on the circumstances, an authorisation may comprise a written application that has been signed by the authorising officer, or an oral application that has been verbally approved by the authorising officer.
Authorising Officer	a person within a public authority who is entitled to grant authorisations under the 2000 or 1997 Acts or to apply to the Secretary of State for such warrants. Should be taken to include senior authorising officers.
CHIS	covert human intelligence sources

Confidential information	**c**onfidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.
Core Functions	the statutory powers and duties given to the Council to investigate activities of private individuals, groups and organisations within its jurisdiction for the benefit and protection of the public
Council	Surrey Heath Borough Council
Crime Threshold	Local Authorities can only authorise the use of directed surveillance to: To prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** relate to the underage sale of alcohol and tobacco. For the purposes of preventing disorder which involves a criminal offence punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment
CSP	Communication Service Provider (a service provider that transports information electronically)
DS	directed surveillance
Gatekeeper	a person with the role of advising on the completion and the quality of applications under RIPA
Handling Code	the code for handling of information
ICD	interception of communication data
Legal privilege	matters subject to legal privilege are defined in section 98 of the 1997 Act. This includes certain communications between professional legal advisers and their clients or persons representing the client.
Member	an employee of an organisation, or a person seconded to that organisation (for example, under the terms of section 24 of the Police Act 1996).
Officer	an officer of a police force, HMRC or the OFT, or a person seconded to one of these agencies as an officer.

OSC		Office of the Surveillance Commissioner which carries out inspections at regular intervals to ensure that RIPA is properly applied
Prescribed Office		those offices, ranks and position prescribed for the purposes of section 30(1) of RIPA for the purposes of granting authorisations under sections 28 and 29 of RIPA
Public authority		any public organisation, agency or police force (including the military police forces).
Private information		any information relating to a person in relation to which That person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation.
RIPA		Regulation of Investigatory Powers Act 2000
RMO		RIPA Monitoring Officer
Secretary of State		any Secretary of State (in practice this will generally be the Home Secretary).
Senior Authorising Officer		**a** person within a public authority who is entitled to grant intrusive surveillance authorisations under the 2000 Act or to apply to the Secretary of State for such warrants. See also Authorising officer
SPoC		Single Point of Contact
SRO		Senior Responsible Officer who is responsible for corporate oversight of the RIPA processes and that all authorising officers are of an appropriate standard. Where an inspection report by the OSC has concerns about the standards of authorising officers, the SRO will be responsible for ensuring the concerns are addressed.
URN	-	the Unique Reference Number stating the year, division and number of each application for authorisation for directed surveillance and CHIS

APPENDIX ELEVEN

Procedure for Judicial Approval

Judicial Oversight

1. The *Protection of Freedoms Act* brought into law the Judicial oversight of all RIPA approvals by Local Authorities. It inserts sections into the 2000 Act which mean that authorisations, whilst still given by LA staff, do not take effect until a Magistrate has approved them. The Judicial oversight does not take the place of the current authorisation process – it is an oversight function and not an authorisation function. **The Authority may not undertake the regulated activity until *Judicial Approval* has been given.**

2. Once the application has been approved by an officer listed in Appendix 1, the Authority must apply to the Magistrates Court for an order confirming that :
    a. the person who granted or renewed the authorisation, or the notice was entitled to do so ;
    b. the grant or renewal met the relevant restrictions or conditions ;
    c. 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
    d. it is still (at the time the court considers it) reasonable to believing the grant / renewal to be both necessary and proportionate.

3. The oversight will be determined at a hearing in front of a single Magistrate. An officer appointed to do so (and listed at Appendix 1A) must approach the court office to arrange the hearing.

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.

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

5. 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 standard of the form and any attachments, the *AO* must submit the bundle electronically to the *RMO* for onward transmission to the courts.

6. The bundle for submission to the courts must include :
    a. the application for the order approving the authorisation ;
    b. the authorised application or renewal form ;
    c. any supporting information that, exceptionally, does not form part of the form ;
    d. any information you have that might show a reason to refuse the application ;
    e. 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 6.1.3 above) ; and
    f. a copy of annexes 1 and 1A to this policy, showing that the *Authorising Officer* and the applicant are both persons duly approved to carry out those functions by the Authority.

The following are things that you should normally disclose to the Court when making your application to them :

- You have made previous applications under RIPA and these have been turned down.
- There have been other investigations into the same subject or at the same address, regardless of 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.

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

7. 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.

8. The applicant must attend the hearing and assert the accuracy of the application. They must also be prepared to answer any questions about the application and the investigation which the Magistrate may have. At the end of the application, the magistrate will give the court's decision.

9. Once the bundle has been submitted, the *RMO* will note this in the Central Record. Within 24 hours of receiving the Court's decision, the Applicant must notify the *RMO* and the *Authorising Officer* by sending them an email. Both parties must also be sent copies of any court order. The original must be retained on the investigation file. The *RMO* will note the record with the outcome.

10. In the event that the Court refuses the application, the applicant, the *Authorising Officer* and the *RMO* will review the decision within 24 hours and decide if they wish to make representations to the Court before a *Quashing Order* is made.

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 submit to the court.
The Magistrate has made a mistake of fact (for example that the offence you are investigating does not meet the seriousness criteria).	Evidence the correct facts and 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 AO 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.

11. If the Authority decides to make representations about a refused application, the *AO* or *RMO* will immediately notify the court officer of this and request a hearing. Grounds for the submission should be set out in writing and notified to the court before the hearing. It must be drafted by the applicant and approved by the *AO*. If must contain the standard declaration a set out above.

12. If the Authority elects to seek a hearing, the applicant, *AO* and *RMO* will attend the hearing. At the conclusion of the hearing, the *RMO* will note the outcome in the Central Record.