Regulation of Investigatory Powers Act 2000

Policy Guidance & Procedure Document

City of Bradford Metropolitan District Council (the Council)

Word Ref;
Lit/rjw/ripa2000coordination/guidancetrainingdocuments\CBMDCPolicyGuidance\RIPA GuidanceJan 2021rw

Joint Author & Editor	Jason Field	First Edition	June 2003
Title:	Solicitor RIPA Coordinator and Monitoring Officer and Single Point of Contact (SPOC)		
		Last Update	January 2024
		Next Update	January 2025

INDEX

Part1Chapter11 RIPA2000 (ATCD)
Appendix 4 – Scenarios for DCS, CHIS and ACD
Appendix 5- Example of central record sheet for DSC and CHIS

CHAPTER 1- POLICY STATEMENT OF THE COUNCIL AND INTRODUCTION TO RIPA

Policy statement

a) **Purpose** – The Council's officers in the course of investigating frauds, breaches of legislation or regulation and in the interest of the safety and well being of the district may be required to undertake covert monitoring operations to gather evidence to present to a court dealing with criminal matters. In doing so those officers must comply with the relevant legislation i.e. RIPA and the associated regulations and codes of practice. Evidence collected without complying with the statutory procedures may become inadmissible before the Courts and prejudice the outcome of an investigation.

b) **Scope** – This policy covers the use of covert CCTV, monitoring equipment such as audio recording, cameras, video cameras, binoculars and covert human intelligence sources (CHIS). RIPA also covers the monitoring of Internet use, telephone use, or postal use where the individual whose actions are being monitored is unaware of the operation. This policy does not contemplate the monitoring of internet use, telephone use or postal use other than in exceptional circumstances as this is unlikely to be necessary and disproportionate in most if not all local authority criminal investigations.

c) **Exclusions** – City centre CCTV operating within defined boundaries and brought to the attention of the public by the use of signs is not covered by this policy.

d) **The procedure** – when a Council criminal investigation (enforcement) officer considers that covert operations are the only method of collecting the evidence required s/he should obtain internal authorisation and court approval for such activity before undertaking any covert surveillance techniques whatsoever and follow the guidance set out in this document as advised by the Council's RIPA coordinator and monitoring officer (RICMO) The Councils RICMO is available to advise on procedure and maintains a central register of all authorisations approvals and refusals.

e) Review of the policy - the policy and guidance document is reviewed annually by the Councils Senior Responsible Officer (SRO) for RIPA in consultation with the Councils RICMO.

6. **Guiding Principles**

6.1 Surveillance is an intrusion into the privacy of the citizen. The Council's officers will not undertake surveillance unless it is necessary and proportionate to the alleged offence and properly authorised and approved where necessary by the magistrate's court. Covert surveillance will not be undertaken without authorization and approval under RIPA to which an absolute defense is provided under s27 RIPA. Where there is an alternative legal means of obtaining the information that is gives rise to less interference with the rights of the citizen, the Council will always take that alternative course rather than undertake covert surveillance.

6.2 Surveillance by covert human intelligence source (CHIS) will not be authorised by the Council other than in exceptional cases due to the potential adverse risk to the health and safety of the investigation officers. A CHIS could exceptionally be authorised when the Councils officer is working alongside the police and after a risk assessment has been approved by the Director of Legal and Governance.

6.3 Covert surveillance will be conducted within the constraints of the authorisation. It will cease when the evidence sought has been obtained or when it becomes clear that the evidence is not going to be obtained by further surveillance. At that point the authorisation should be cancelled.

6.4 In every instance where surveillance is authorised the officer who conducts surveillance will consider and make plans to reduce the level of collateral intrusion into the privacy of third parties.

6.5 All outstanding surveillance authorisations should be reviewed at least monthly and cancelled where there is no further need for surveillance.

6.6 All officers involved in applying for, authorising or undertaking surveillance will understand the legal requirements set out in RIPA and the codes of practice. They will personally take responsibility for ensuring the propriety of their involvement.

6.7 All authorisations, notebooks, surveillance logs and other ancillary documentation that relates to surveillance will be maintained to the required standards and retained for **three years**. All documentation will be volunteered for any management or regulatory inspection on demand.

6.8 Any failure of any part of the process will be brought to the attention of the investigation manager. S/he will consult the Councils RICMO to determine what action should be taken.

6.9 Willful disregard of any part of RIPA, codes of practice or of internal procedures shall be a breach of discipline and subject to the Council's disciplinary code.

6.10 **Surveillance equipment.**

(i) The Council have a considerable amount of technical equipment which can carry out covert surveillance of operations e.g. Cameras, video cameras, binoculars, zoom lenses CCTV and noise tape recording equipment.

(ii) Bearing in mind that such equipment can be used by officers without supervision once authorisation has been granted continued monitoring and thus a record of the use of such equipment requires to be maintained i.e. its return to storage immediately once the covert surveillance has been undertaken.

(iii) Schedules of equipment are kept and updated by enforcement team managers for each Council department which undertakes surveillance either covert or otherwise. The schedule should be reviewed annually by the Councils RICMO.

(iv) In order to effectively monitor the use of the equipment each separate piece of equipment is listed with it reference/serial number and its whereabouts.

(v) The responsibility to monitor the day to day use of such equipment by Council Enforcement officers is primarily that of each enforcement team manager of head of service.

(vi) Included in this guidance are those departments that use surveillance equipment but such surveillance is deemed to be an exception to RIPA2000 e.g. Environmental services (noise monitoring where the person investigated is on written notice the noise is to be monitored and parks and landscapes who use of published motor bike mounted video camera for surveillance over general hot spots for crime rather than individual known suspects. Any other static CCTV equipment which is used overtly i.e. made aware by the Council to the public or its staff by the use of signs indicating its existence does not require authorization or court approval. Such CCTV equipment exists in the Bradford City Centre, the City Hall and the Payroll office security vehicles to name some uses.

6.11 Willful disregard of any part of RIPA, codes of practice or of internal procedures shall be a breach of discipline and subject to the Council's disciplinary codes.

7. Serious crime restrictions and magistrates court approval.

a) It is noted from the 1st November 2012 due to statutory regulation all authorisations under RIPA 2000 for Directed Surveillance and Communications Data may only be granted in respect of ''serious crime'' as defined i.e. a criminal offence carrying a penalty of 6 months or more imprisonment. Council policy is to apply the serious crime test to CHIS investigations.
b) Also from the 1st November 2012 all authorisations granted by the Councils authorised and designated officers of which are the Councils Chief Executive and the Councils Director of Legal and Governance (in consultation with the Leader of the Council) or their authorised deputies can not take effect until it has been approved by a magistrate upon application by the Council.
c) The procedure to be followed is similar to applying for a warrant to enter premises under relevant statutory powers.
d) The application to the Magistrates Court will be made in person usually by a Council solicitor advocate together with the applicant for the authorisation.

e) The existing authorisation for which approval is required will be submitted to the court in writing and with the approval application form completed under cover of a letter before the application for approval is heard formally before the court.
f) This statutory restriction was effectively part of the Councils existing policy in the context of use of RIPA to more serious crime.
g) This policy already acknowledges RIPA should not be used for non serious crime e.g. dog fouling, school's admissions and littering offences as has been so severely critisised in the press and by the Courts

8. Evidence gathering techniques through use of the Internet. The Councils resolved in April 2015 that: -The City Solicitor provides a report/protocol to the Committee on the implications relating to the undertaking of social media criminal investigations.

ADOPTED PROTOCOL/ GUIDANCE JUNE 2016

The Use of Social Networks in Investigations

1. Use of this Guidance

a) This document provides guidance to Council officers who use "open source" social networks to gather information about individuals or groups of individuals in support of any investigation carried out on behalf of the Council, including criminal, civil, child protection and employment investigations. "Open source" means that the information available is not protected by privacy settings and is openly available to anyone that wishes to view it.

b) This guidance does not facilitate the viewing or gathering of information from sources or profiles that are not "open source" and are protected by privacy settings.

c) For example, a Face book profile where a friend request must be accepted before a profile can be viewed would not be an "open source" profile.

d) Access to such information and the gathering of such information requires particular consideration under the Data Protection Act (DPA) 1998, Human Rights Act (HRA) 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000. If such activity is proposed legal advice should always be sought in advance and without that advice is contrary to Council policy.

e) This guidance supplements the Council's Data Protection Policy which supports the delivery of the Information Governance Framework. The guidance should be read alongside the Council's RIPA Policy Guidance and Procedure referred to above.

2. Use of "Open Source" Social Networks

a) “Open source” social networks have become a large accessible source of information about individuals. The information placed on these networks has the potential to be accessed, acquired, used and retained by council officers on behalf of the Council, in particular by investigators seeking evidence to support criminal and civil investigations, defend actions brought against the Council, assist in child protection matters or support employee disciplinary matters.

b) In an annual report the Chief Surveillance Commissioner has stated his view that just because such material is out in the open, does not render it fair game.

c) The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA.

d) Whilst the viewing only of publicly available information, without gathering, storing or processing material or establishing a relationship with the individual is unlikely to engage an individual’s right to privacy under the European Convention on Human Rights , where activities involve officers creating a record of personal data or private information, this activity must be justified with reference to the DPA and HRA to ensure that the rights of the individual have been respected and to ensure that ensuing proceedings are based upon admissible evidence.

3. RIPA, Covert Human Intelligence Sources & Directed Surveillance

3.1 Covert Human Intelligence Source (CHIS)

a) There may be circumstances where activity on social networking sites amounts to the use of a CHIS which would require an authorisation under RIPA. The term CHIS is used to describe people who are more commonly known as informants. The use or conduct of a CHIS would include work by officers working “undercover” whereby a covert relationship is established with another person. Such activity may arise if investigators are seeking to form covert relationships on social networking sites to circumvent privacy settings that have been put in place.

b) Many sources volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by the council. For example, a member of the public volunteering information about something they have viewed on a social network, where a relationship will not have been established or maintained for a covert purpose, will not amount to CHIS activity. This information may be processed by the Council in accordance with the DPA.

c) Further information about the use of CHIS can be found in the Council’s RIPA Policy, Guidance and Procedure.

d) If officers believe that proposed use of social networks may involve the use of a CHIS, legal advice should be sought and any CHIS activity must be authorised in accordance with the Council’s RIPA policy.

3.2 Directed Surveillance

a) The Chief Surveillance Commissioner has expressed the view that the repeated viewing of open source sites for the purpose of intelligence gathering and data collation or a single trawl through large amounts of data ("data mining") could amount to activity for which a RIPA authorisation for Directed Surveillance should be sought, where the serious crime threshold is met.

b) Where private information is being gathered by officers from social networks to support a criminal investigation for an offence that attracts a maximum sentence of 6 months or more and the proposed use of the social network meets the definition of Directed Surveillance, authorisation must be sought in accordance with the Council's RIPA policy. Officers are advised to seek legal advice on such proposed activity.

c) Where information is gathered by officers from open source sites that would require a RIPA Authorisation for Direction Surveillance if it were not for the serious crime threshold then no further covert surveillance must be undertaken in accordance with the Council's RIPA Policy, Guidance and Procedure.

d) Where individuals volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by the council, this activity will not amount to Directed Surveillance and the information may be processed by the council in accordance with the DPA.

3.3 Surveillance of Employees

a) Covert surveillance of an employee as part of a disciplinary process may not amount to Directed Surveillance for the purposes of RIPA as this is an "ordinary function" of the council rather than a "specific public function" or ''core function'' as described in R V Police 2008

b) Where online covert surveillance involves employees then the Information Commissioner's Office's (ICO) Employment Practices Code (part 3) will apply.

c) This requires an impact assessment to be done before the surveillance is undertaken to consider, amongst other things, necessity, proportionality and collateral intrusion. Whilst the code is not law, it will be taken into account by the ICO and the courts when deciding whether the DPA has been complied with (see section 3 below).

d) Where individuals volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by the council, this activity will not amount to covert surveillance and the information may be processed by the council in accordance with DPA.

e) In any event the Council policy does not permit covert surveillance unless authorised under RIPA.

4. Data Protection Act 1998 (DPA) and the General Data Protection Regulations 2018 (GDPR)

a) The provisions of the DPA and associated Regulations i.e. GDPR apply to all personal data processed by the Council, including personal data acquired from open source social network sites. Personal data must only be processed in accordance with the DPA and the Council's DP policy.

b) All personal data must be processed fairly and lawfully and the processing of personal and sensitive personal data must be justified under one or more of the fair processing conditions set out in Schedules 2 and 3 of the DPA and the GDPR.

c) The Council strives to adopt the least intrusive approach to the delivery of council services and any processing must be necessary and proportionate in order to be justified under one of the fair processing conditions. "Necessary" means more than simply convenient or desirable for the Council, where processing corresponds to a "pressing social need".

d) "Proportionate" means that the Council needs to try and strike a fair balance between the rights of the data subjects, and the legitimate aims of the Council. This means the data collected to support investigations must not be excessive and must take account of the particular circumstances of the data subject.

e) Officers must also consider whether the use of open source social networks as part of an investigation is likely to result in collateral intrusion and the personal data of uninvolved third parties being processed by the Council. The processing of third party data must also be justified under the DPA with reference to the fair processing conditions.

f) If officers are unsure as to whether processing is justified under the DPA, advice can be sought from the Directorate Data Practitioner, the Corporate Information Governance Team or Legal Services.

5. Human Rights Act 1998

a) Article 8 of the European Convention on Human Rights (ECHR) which was brought into force by the HRA provides that an individual's rights to family and private life may only be interfered with where the interference is in accordance with the law and necessary for one of a number of legitimate purposes including public safety, the prevention of crime or disorder, the protection of health and morals, or the protection of the rights and freedoms of others. In order to meet the requirement of necessity the interference must be proportionate to the legitimate purpose.

b) The case law recognises that the concept of "private life" is wide ranging. The test to be applied in determining whether Article 8 rights are engaged is whether there is a "reasonable expectation of privacy".

c) This is a broad question that must take into account all the circumstances of the case. The creation of a permanent record from information currently in the public domain or the systematic retention of information may engage an individual's Article 8 rights.

d) The Supreme Court has now confirmed that the state's systematic collection and storage in retrievable form even of "public" information about an individual is an interference with private life. Therefore, the requirements of lawfulness, necessity and proportionality should be considered by officers whenever information about individuals from social networks is acquired, used, or retained.

e) Given the need to consider issues of lawfulness, necessity and proportionality in order to justify the processing of personal data under the DPA, where the processing of personal data from open source social networks is justified under the DPA, any interference with the individual's right to privacy under Article 8 through the processing of that data will also be justified.

f) In order to comply with Article 8 consideration must also be given to any collateral intrusion that might occur and result in private information being obtained about uninvolved third parties, whether this intrusion is lawful, necessary and proportionate and how it can be avoided, minimised or mitigated.

6. Use of Corporate Accounts

a) Investigations using social networks should only be conducted using Corporate Accounts created for the purpose of carrying out such investigations. Accounts must be approved by your line manager and by your service area digital champion.

b) You can find out who your digital champion is in the related documents section and more about the process of applying for an account in the 'general' toolkit guidance.

1. **INTRODUCTION**

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a legal framework for the control and regulation of surveillance and information gathering techniques that Public Bodies undertake in the conduct of their duties. The need for such control arose from the enactment of the Human Rights Act 1998 (HRA) and more specifically Articles 6 and 8 of the European Convention of Human Rights. Article 8 states:

ARTICLE 6 RIGHT TO A FAIR TRIAL; AND

ARTICLE 8 RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1) *Everyone has a right to affair trial including the investigation of the matter potentially subject to a trial AND the right to respect for his private and family life, his home and his correspondence.*

2) *There shall be no interference by a public authority with the exercise of these rights except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The right to a fair trial is an absolute right and the right to respect for private and family life is a qualified right' Public authorities'' can lawfully interfere with Article 8 for the reasons given in part 2 of Article 8. It is RIPA that provides the legal framework for such lawful interference.

Scope of this Procedure Document

The Act provides a permissive regime for surveillance and information gathering techniques undertaken by all public bodies including the Intelligence Services, Police, Armed Forces, Customs and Excise and Local Authorities.

This document is intended to cover the surveillance and information gathering techniques which are most appropriate to local authority work. In this context this also includes the investigation of internal fraud e.g. Directed surveillance (DS) and covert human Intelligence source(s) (CHIS) and Data Communications data (DC) gathering.

From the 1st November 2012 due to statutory regulation that authorisations under RIPA 2000 for DS and DC can only be granted in respect of ''serious crime'' as defined i.e. carrying a penalty of 6 months or more imprisonment.

Also from the 1st November 2012 all authorisations granted by the Councils authorised officers and designated officers of which are only the Councils Chief Executive and the Direcor of Law and Governance in consultation with the Leader of the Council do not take effect until they have been approved by a magistrate upon application by the Council.

The procedure to be followed is similar to applying for a warrant to enter premises.

This will be made in person usually by a Council solicitor advocate together with the applicant for the authorisation.

The existing authorisation for which approval is required will be submitted to the court in writing under cover of a letter either by secure email or by hand before the application for ratification is heard formally before the court.

An inconsistency now appears between the 3 covert surveillance techniques which can be undertaken by a local authority. The serious offence test applies only to directed surveillance. It does not apply to the covert techniques of a covert human intelligence source and Data communication.

However, Council policy is to apply the serious offence test applied statutorily to DS to the CHIS and DC's techniques.

Some techniques listed below, are not regularly undertaken by local authorities in relation to members of the public, but would also come within the scope of RIPA. Those techniques are not covered in detail in this document.e.g.

- The interception of any communication such as postal, telephone or electronic communications without both the sender and receiver's permission.
  (See below for details of new powers to obtain information about communications from communications services providers)

- The covert use of surveillance equipment (intrusive surveillance (IS) within any premises or vehicle, including business premises and vehicles, with the intention of covertly gathering information about the occupant/s of such premises or vehicles, unless undertaken as part of a CHIS[1] authorisation.

- The use of any person, other than an employee of the Council or agent, to establish or use a **covert relationship**[2] with another person in order to gather, disclose or disseminate information which results from that relationship in the conduct of local authority business.

- The use of any person under the age of 18, whether or not an employee of the Council, to establish or use a covert relationship with another person in order to gather, disclose or disseminate information which results from that relationship in the conduct of local authority business. (See S.I. 2000 No. 2793 – The Regulation of Investigatory Powers (Juveniles) Order 2000

- The control and disclosure of information held on computer or paper records covered by the Data Protection Act or Freedom of Information Act.

If it is intended to carry out such activity further guidance should be sought from the Councils RIPA monitor and co-coordinator in Legal Services (see Appendix 1).

---

[1] See later guidance on Covert Human Intelligence Sources (CHIS).
[2] Further guidance on the interpretation of text highlighted in bold can be found in the Glossary of Terms.

The interference of telecommunications sent and received by staff is mentioned in chapter 3 below

Local authorities are restricted in the type of surveillance and information gathering techniques that they can be authorised to undertake under RIPA. These are contained within Part I Chapter II and Part II of the Act and relate to **surveillance** and the use of covert human intelligence sources (CHIS) and access to communications data.

Part II of the Act came into force on 25 September 2000 and therefore all investigations which involve covert surveillance or the use of CHIS after this date should be undertaken in accordance with the authorisation procedures contained in this document. Failure to obtain an authorisation is likely to be deemed to be unlawful under the HRA and is liable to be ruled inadmissible in Court. It is strongly recommended that authorisation is obtained where it is likely to obtain **private information** using covert surveillance techniques or CHIS, whether or not that person is the target of the investigation. The Act not only covers the observation of members of the public but would also cover the observation of staff and members as part of an internal investigation.

This document does not address the assessment of risks that officers might encounter during investigations. Normal departmental policies on identifying such risks should be adopted if it perceived that any risk might arise from a specific operation. The CHIS authorisation form in Appendix 3 at section 8 specifically refers to risk assessment.

2.4 The Investigatory Powers Commissioners Office (IPCO) and the Investigatory Powers Act 2016 (the 2016 Act)

The Government appoints a **Surveillance Commissioner** and his/her office (IPCO) to review how Public Authorities implement the requirements of RIPA. The Commissioner has wide ranging powers of access and investigation. The Council receives periodic inspection from the Commissioners staff and therefore it is essential that everyone who engages in RIPA type activities is fully aware of the law and this procedure.

The Investigatory Powers Commissioner.

The Investigatory Powers Commissioner and his/her Judicial Commissioners are responsible for overseeing the use of investigatory powers by public authorities which include law enforcement, the intelligence agencies, prisons, local authorities and other government agencies (e.g. regulators). In total over 600 public authorities and institutions have investigatory powers.

The Commissioners are supported in this work by a body of civil servants – the Investigatory Powers Commissioner's Office (IPCO)

The more intrusive powers such as interception, equipment interference and the use of surveillance in sensitive environments will be subject to the prior approval of a Judicial Commissioner. Use of these and other surveillance powers, including the acquisition of communications data and the use of covert human intelligence sources, are also overseen by a programmed of retrospective inspection and audit by Judicial Commissioners and IPCO's inspectors.

IPCO assumed the responsibility for oversight of investigatory powers from the Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (IScomm) in September 2017 under the 2016 Act. IPCO immediately takes over the inspection and audit functions of these bodies and the prior approval function of Surveillance

Communications Data Code of Practice Nov 2018 (Extract) page 51

Para 8 Further restrictions and requirements in relation to applications Local authority procedures

8.1 The National Anti-Fraud Network ('NAFN') is hosted by Tameside Metropolitan Borough Council.

8.2 In accordance with section 73 of the Investigatory Powers Act 2016(the Act), all local authorities who wish to acquire communications data under the Act must be party to a collaboration agreement. In practice this means they will be required to become members of NAFN and use NAFN's shared SPoC services. Applicants within local authorities are therefore required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinize the applications independently. They will provide advice to the local authority ensuring it acts in an informed and lawful manner.

8.3 Such collaboration agreements are required to be certified by the Secretary of State in accordance with section 73(3)(c). Where a collaboration agreement is considered to both meet the needs of those authorities' party to it and to assist in the effective application of the relevant provisions and safeguards detailed in the Act, including in relation to the factors listed in the section on collaboration agreements below, the Secretary of State will certify the agreement, therefore allowing the relevant local authorities to acquire communications data.

8.4 Certified collaboration agreements will be subject to review by the Secretary of State at least every three years. Authorities party to the collaboration agreement are required to notify the Secretary of State of any changes which may necessitate an earlier review.

8.5 In addition to being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the local authority is aware the application is being made before it is submitted to an authorizing officer in OCDA. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations. Where the verifying officer is employed by a local authority other than that which requires access to communications data, the verifying officer must also be of an appropriate rank.

8.6 NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

8.7 A local authority may not make an application that requires the processing or disclosure of internet connection records for any purpose

A Tribunal system through the Investigatory Powers Tribunal (IPT) has been set up to deal with complaints from any person who considers that a Public Authority has breached a Convention Right in contravention of the HRA. The Home Office has published a set of information leaflets on this topic. Copies have been sent to all Council public offices. These should be available to the public at all times.

CHAPTER 2 COVERT SURVEILLANCE

There are two categories of **covert surveillance**:

- Intrusive Surveillance, and
- Directed Surveillance.

Intrusive Surveillance

Intrusive surveillance is defined as covert surveillance that:

a) is carried out in relation to anything taking place on any **residential premises** or in any **private vehicle**; and

b) Involves the presence of any individual on the premises or in the vehicle or is carried out by means of a **surveillance device**.

If the device is not located on the premises or in the vehicle, it is not intrusive surveillance unless the device consistently provides information of the same quality and detail as could be expected to be obtained from a device actually present on the premises or in the vehicle.

OFFICERS OF A LOCAL AUTHORITY CANNOT AUTHORISE INTRUSIVE SURVEILLANCE.

Operations that involve intrusive surveillance are limited to the Intelligence Services, Armed Forces, MOD, Police and HM Customs and Excise. The majority of covert surveillance undertaken by local authority officers would fall within the category of Directed Surveillance.

If it is considered that surveillance that is intended to be undertaken may fall with the scope of intrusive surveillance, then further guidance should be sought from the Councils RIPA Coordinator.

Directed Surveillance

Directed Surveillance (DS) [referred to in this document as Directed Covert Surveillance (DCS)] is defined as surveillance which is covert, but not intrusive, and undertaken:

a) for the purpose of a specific investigation or operation;

b) in such a manner as is likely to result in the obtaining of **private information** about a person (whether or not that person is the target of the investigation or operation); and

c) In a planned manner and not by way of an **immediate response** whereby it would not be reasonably practicable to obtain an authorisation prior to the surveillance being carried out.

The flowchart at Appendix 2 and the scenarios in Appendix 4 provide some guidance on when an authorisation for DCS would be required.

It should be noted that it is irrelevant where the subject of the DCS is when he is being observed. E.g. at work/home/in public places.

Covert Human Intelligence Sources (CHIS)

NB the statutory definitions of DCS and IS and CHIS are separate and distinct and do not in any way overlap e.g. the presence of a CHIS on residential premises is not by definition intrusive surveillance.

The term Covert Human Intelligence Source (CHIS) is used to describe people who are more commonly known as informants and are used more widely by the Police and other similar organisations than by Local Authorities. However, CHIS would also include work by officers working "undercover" whereby a covert relationship is established with another person. Such activity may be undertaken by local authority officers.

This document only relates to situations when a CHIS authorisation would be required for undercover work by local authority officers owing to the infrequent and exceptional circumstances when someone other than a local authority employee would be used. If any officer contemplates using any person who is not an employee of the Council as CHIS, then they should contact the Councils RIPA Co-coordinator for further advice before proceeding.

A person is a CHIS if:

(a) s/he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) s/he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) S/he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

The flowcharts at Appendix 2 and the scenarios at Appendix 4 provide some guidance as to when an authorisation for use of a CHIS is required.

N.B. If a CHIS uses surveillance equipment in the conduct of his/her covert activity, a separate authorisation for DCS is required. This would also apply to situation when the recording device is being used within a private residence or vehicle if the CHIS had been invited into the residence or vehicle. The Council does not have any specialist equipment.

It is considered that a typical test purchase exercise that does not go beyond what would be considered to be a normal transaction would not be considered as a CHIS activity. Thus it appears that the covert surveillance of a private hire driver by a local authority

licensing officer as a secret passenger who has not pre booked the private hire vehicle may fall within a CHIS.

CHAPTER 3 ACCESS TO TELECOMMUNICATIONS DATA (ACoD)

Introduction

Section 60A of the Investigatory Powers Act 2016 empowers all local authorities to acquire information defined as **communications data**. This includes **subscriber data** and **service data** but not **traffic data** as defined by the 2016 Act. By way of examples the Council could seek details of a subscriber name and address i.e. subscriber details. If the Council required information of specified telephone numbers called and calling the subscriber or web-addresses visited, then this is service data.

A standard form for requesting an authorisation to seeking communications data is in the appendices and the Code of Practice is available from the SPOC officer.

The authorisation and approval procedure is similar to that described for directed surveillance and is explained below but must be via the National Anti-Fraud Network (NAFN).

The NAFN officer appointed as SPOC amongst other things carries out a quality control role and advises the Investigating Officer and the Authorising Officer on various matters as follows i.e.

Whether the application meets the statutory requirements,

Whether the information being sought can be easily obtained by the Communications Service Providers (CSP) or Internet Service Providers (ISP) and

Whether the application would be cost effective. The S.P.O.C will also be the contact officer for all liaisons with CSPs and ISPs.

Both historical and future information may be sought from a provider subject to limitations. The Councils RIPA coordinator was accredited to act as a SPOC by the Home Office in September 2004.

All communications data with be sought through the National Anti- Fraud Network (NAFN) of which Bradford Council is a member and pays an annual subscription. This public organisation is based at the Councils of Tameside and Brighton and Hove.

1. The law practice and procedure for obtaining Communications data through the Councils SPOC and NAFN (Tameside Council).

.

Provisions under Investigatory Powers Act 2016

[60A. Power of Investigatory Powers Commissioner to grant authorisations (1) Subsection (2) applies if the Investigatory Powers Commissioner, on an application made by a relevant public authority, considers—
(a) that it is necessary for the relevant public authority to obtain communications data for a purpose falling within subsection (7),
(b) that it is necessary for the relevant public authority to obtain the data— (i) for the purposes of a specific investigation or a specific operation, or (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, and
(c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.
(2) The Investigatory Powers Commissioner may authorise the relevant public authority to engage in any conduct which— (a) is for the purpose of obtaining the data from any person, and (b) relates to— (i) a telecommunication system, or (ii) data derived from a telecommunication system.
(3) Subsections (1) and (2) are subject to— (a) section 62 (restrictions in relation to internet connection records), (b) sections 70, 73 and 75 and Schedule 4 (restrictions relating to certain relevant public authorities), (c) section 76 (requirement to consult a single point of contact), and (d) section 77 (Commissioner approval for authorisations to identify or confirm journalistic sources).
(4) Authorised conduct may, in particular, consist of the relevant public authority—
(a) obtaining the communications data itself from any person or telecommunication system,
(b) asking any person whom the relevant public authority believes is, or may be, in possession of the communications data or capable of obtaining it—
(i) to obtain the data (if not already in possession of it), and Investigatory Powers Act 2016
(ii) to disclose the data (whether already in the person's possession or subsequently obtained by that person) to the relevant public authority, or
(c) requiring by notice a telecommunications operator whom the relevant public authority believes is, or may be, in possession of the communications data or capable of obtaining it—
(i) to obtain the data (if not already in possession of it), and
(ii) to disclose the data (whether already in the operator's possession or subsequently obtained by the operator) to the relevant public authority.
(5) An authorisation—
(a) may relate to data whether or not in existence at the time of the authorisation,
(b) may authorise the obtaining or disclosure of data by a person other than the relevant public authority, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned, and
(c) may, in particular, require a telecommunications operator who controls or provides a telecommunications system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system.
(7) It is necessary to obtain communications data for a purpose falling within this subsection if it is necessary to obtain the data—
(a) in the interests of national security,
(b) for the applicable crime purpose (see subsection (8)),
(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
(d) in the interests of public safety,
(e) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
(f) to assist investigations into alleged miscarriages of justice, or
(g) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition— (i) to assist in identifying P, or (ii) to obtain information about P's next of kin or other persons connected with P or about the reasons for P's death or condition.
(8) In subsection (7)(b), "the applicable crime purpose" means— (a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime; (b) in any other case, the purpose of preventing or detecting crime or of preventing disorder.
(9) The fact that the communications data which would be obtained in pursuance of an authorisation relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that it is necessary to obtain the data for a purpose falling within subsection (7).
(10) See— (a) sections 70 and 73 for the meaning of "relevant public authority"; (b) section 84 for the way in which this Part applies to postal operators and postal services; (c) section 86(2A) for the meaning of "serious crime". Investigatory Powers Act 2016

1 Notes 1 Added by Data Retention and Acquisition Regulations 2018/1123 reg.5 (February 5, 2019 being the commencement date)

Section 73 Local authorities as relevant public authorities

(1) A local authority is a relevant public authority for the purposes of this Part [but only so far as relating to authorisations under section 60A] 1 . (2) […]2 [(3)

An authorisation may not be granted under section 60A on the application of a local authority unless—
(a) section 60A(1)(a) is met in relation to a purpose within section 60A(7)(b),
(b) the local authority is a party to a collaboration agreement (whether as a supplying authority or a subscribing authority or both), and

(c) that collaboration agreement is certified by the Secretary of State (having regard to guidance given by virtue of section 79(6) and (7)) as being appropriate for the local authority. [(3A) In subsection (3)— "collaboration agreement" means an agreement under section 78 that falls within subsection (1)(b)(iii) of that section, "subscribing authority" has the same meaning as in section 78, "supplying authority" has the same meaning as in section 78.] 4] 3 (4) -(7) […]2 Notes 1 Words inserted by Data Retention and Acquisition Regulations 2018/1123 Sch.1 para.13(2) (February 5, 2019 being the commencement of 2016 c.25 s61(1)

1.1 The 2016 Acts provisions draw a distinction between interception of communications in the course of their transmission, which is activity excluded for local authorities, and conduct involving the obtaining or disclosure of communications data, which is activity permitted for local authorities.

1.2 Conduct to obtain communications data is lawful in response to a properly authorised notice or authorisation. There is no liability for a breach of the human right to ‘’ privacy and a family life ‘’attached to actions undertaken as a result of a requirement or authorization under the 2016 Act

Definition of Communications Data

1.3.1 “Communications data is information held by communication service providers (e.g. telecom, internet and postal companies) relating to the communication made by their customers”

1.3.2 “The term communications Data embraces the who, what and where of a communication but not the content”

1.3.3 The definition therefore includes information relating to the use of a communications service but does not include the contents of the communication itself.

Example:

- In the context of a letter it will include the information on the envelope but not the contents of the letter. The information will therefore include the name and address of the recipient and the postmark showing when and where the letter was sent. It might also contain details of the address of the sender if recorded on the envelope.
- In the context of telephone data, it would include the telephone numbers of the phone from which the call was made and the number of the phone receiving the call. It also includes the date, time, duration and place of the call. It does not include the actual content of the telephone call.
- As regards e mail and internet it would include details of the subscriber account. It also includes dates and times when e mails have been sent or received. The content of the e mails is excluded from Communications Data. The web sites are included but not the actual web pages that have been viewed.

It is broadly split into 3 categories:

"traffic data"; this is usually data generated by the CSP in the process of delivering a communication. (Not included in LA authorisation)
Server use or billing information) the use made of the service by any person i.e.

Itemised telephone records;
e.g.
Numbers called
Itemised connection records
Itemised timing and duration of services
Connection, disconnection and reconnection information
Provision and use of forwarding/redirecting services
Conference calls call messages call waiting & call baring information

Postal records including records of:

Registered, recorded or special delivery postal items
Parcel, consignments, delivery and collection
Information about the provision and use of forwarding/redirection services

Internet log on history

e.g. E mail logs (sent and received), web pages visited

Subscriber information) other information (not in a) or b) above) that is held or obtained by an operator on a person they provide a service
e.g.
Subscriber account information
Name and address for information and billing: including billing arrangements i.e. method of payment.
Collection/delivery arrangements for a PO Box (i.e. whether it is collected or delivered. It does not include details of where it is collected from or delivered to)
Abstracts from personal records provided by the subscriber to the service provider. This does not include password details.
Mobile/landline tel number
Fax number
SIM card number
E mail address
PO Box number
Name & address.

NB: If LA's require Server use information and Subscriber information separate applications for are required for each type of information

Sources of information
1.4.2Telecom Providers (CSP's)

- Landline phone services providers

(E.g. Vodafone, Orange, O2 (UK), T-Mobile)
- Mobile service providers
  (E.g. BT, Telewest, Cable & Wireless, NTL)

Internet Providers (ISP's)

(E.g. BT, AOL, Telewest, NTL)
- Virtual ISP's
  (E.G. Wanadoo [Energis], Demon [Thus], Cable & Wireless)
- Portals
  (Hotmail, Yahoo, Lycos)

Postal Services Providers

(E.g. Royal Mail, Parcel-force, DHL)

Other knowledge investigators may find useful.

Mobile phone components

- Handset (with a unique IMEI number)
- Sim Card
- Mobile Number
-

International Mobile Equipment Identifier (IMEI)

This is an identification number chosen by the manufacturer. It has at least 15 digits denoting the serial number, code relating the approved home country of use, the final assembly code

The Sim card (Subscriber Identity Module)

This card contains a 20-digit serial number. It should be remembered that the SIM card can be moved between hand sets (subject to compatibility) it is the SIM card which is the device which contains information relevant to the customer.
To obtain information about the customer the first step is to identify the service provider from whom this information can be sought. This is to be found in the 20-digit serial number. The forth and 5th digits identify the service provider. The main UK service providers are numbered as follows:

10=Vodaphone
11=02
12=Orange
13=T Mobile

Having identified the service provider, the next step is to identify the subscriber details. These are to be found in the International Mobile Subscriber identity number that is also included in the SIM number.

International Mobile Subscriber identity (IMSI)

This is in the last 15 digits of the SIM card. The first three digits relate to the country and are known as the Mobile Country Code. The next two digits identify the operator within the country and are referred to as the Mobile Network Code. The final digits (no more than 10) identify the individual subscriber. These are known as the Mobile Station Identification Numbers. Having identified the service provider and the MSIN number it is then possible to identify the subscriber.

Mobile telephone numbers.

Sometimes the only evidence that is likely to lead the investigating officer to the offender is the mobile telephone number. This has occurred when for example illegally deposited waste identifies a person living at a named address. The only information that may lead to the identity of the culprit is a vague description and an unsolicited leaflet referring to a mobile telephone number. The mobile phone number is capable of leading the officer to the subscriber because it is unique to the subscriber and the service provider. The first five digits relate to the service providers network and the last 6 digits are the individual subscriber number. These numbers are not conclusive as personal telephone numbers can be transferred from one network to another. Details of the service provider can be found by entering the first five digits on the display page at www.magsys.co.uk and pressing the 'enter' key on your keyboard.

Obtaining and Disclosing Data

Necessity test:
1.5 A strict test of "necessity" must be met before any communications data is obtained under Chapter II. The authorising officer must not only consider the communications data to be necessary but must also consider the conduct involved in obtaining the communications data to be "proportionate". The grounds on which it is necessary are:

In the interests of national security;

For the purpose of preventing or detecting crime or of preventing disorder; (This is the only ground currently available to Local Authorities for accessing communications data
In the interests of the economic well-being of the United Kingdom;
In the interests of public safety;
For the purpose of protecting public health;
For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

Methods of acquiring data:

1.6 There are ways to obtain communications data. Firstly, an authorization must exist. This provides a legal basis upon which the Law enforcement agency (LEA) may collect the communications data themselves if the data provider cannot provide it.

1.7 The second way is by a notice served by the Law enforcement agency (LEA) upon the holder of the data, requiring them to comply with the terms of the notice.

Level of Authorisation:

1.8 The appropriate level of officer i.e. a SPoic within NAFN

Proportionality test (C/F the human rights infringed)

1.9 The NAFN Spoc must also consider the conduct involved in obtaining the communications data to be proportionate. Proportionality is a crucial concept. In both the 2016 Act and the 2018 code reference is made to the conduct being proportionate. This means that even if a particular action which interferes with a Convention right is for the purpose of pursuing a legitimate aim (as listed in Para 4.1 of the code) this will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any interference with a Convention right should be carefully designed to meet the objective in question and must not be arbitrary or unfair. Even taking all these considerations into account, in a particular case the interference may still not be justified because the impact on the individual or group is too severe.

When an authorization may be appropriate:

1.10 In order to illustrate, an authorisation may be appropriate where:
The postal or telecommunications operator is not capable of collecting or retrieving the communications data;
It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

Applications to obtain communications data under the Act
1.12 The application form is subject to inspection by the Commissioner and both applicant and designated person may be required to justify their decisions. Applications to obtain communications data under the Act should be made on a standard form (paper or electronic) which must be retained by the public authority (see section 7 of the code) and which should contain the following minimum information:
– **The name** (or designation) of the officer requesting the communications data;
The operation and person (if known) to which the requested data relates;
– **A description**, in as much detail as possible, of the communications data requested (there will also be a need to identify whether it is communications data under section of the Act);
– **The reason** why obtaining the requested data is considered to be necessary for the purpose in paragraph 1.5 above (the relevant purpose also needs to be identified);

– **An explanation** of why obtaining the data constitutes conduct proportionate to what it seeks to achieve;
Where appropriate, a consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified; and
– The **timescale** within which the communications data is required. Where the timescale within which the material is required is any greater than routine, the reasoning for this to be included.

1.13 **The Authorisation Process:**
The application form is sent to NAFNs Spoc who will record whether access to communications data was approved or denied, by whom and the date. If the form is rejected the SPOC will issue a rejection form (in home office approved format) which is sent to the applicant. If the application is accepted the application form can be marked with a cross-reference to the relevant authorisation or notice.

Review/ Renewal:
1.14 Authorising officers should specify the need for reviews, there frequency and who should carry out the reviews. This should be done at the time of the authorisation. The identity of the reviewing officer will reflect the degree of potential collateral intrusion. The review process is required as a matter of good practice. It is not a statutory requirement. It is however a statutory requirement that there is a renewal within a month of a continuing Notice or Authorisation.
Content of an authorisation
1.15 An authorisation itself can only authorise conduct to which the relevant sections of the 2016 Act apply.
n:
- A description of the conduct to which the 2016 Act applies that is authorised;
- The purpose in paragraph 1.5 above the data is required; and
- The name (or designation) and office, rank or position of the designated person.

1.16 The authorisation *should* also contain:
- A unique reference number.
- A description of the communications data required;
- An explanation as to why the data is proportionate to what it seeks to achieve
- A consideration as to why the data cannot be gathered by less intrusive means
- A consideration of collateral intrusion, i.e. the possibility the privacy of others may be invaded and why that risk is justified.
- The time scale within which data is required.
Content of a notic

- A description of the required communications data;
- The purpose in paragraph 1.5 above the data is required;
- The name (or designation) and office, rank or position of the designated person;
- The manner in which the data should be disclosed.

1.18 The Notice *should* also contain:
- A unique reference number;
- **An indication of any urgency** (where appropriate);
- A statement stating that data is sought under the provisions of Chapter II of Part I

Of the Act. I.e. an explanation that compliance with this notice is a legal requirement;
- Contact details so that the veracity of the notice may be checked.
- An explanation as to why the data is proportionate to what it seeks to achieve
- A consideration as to why the data cannot be gathered by less intrusive means
- A consideration of collateral intrusion, i.e. the possibility the privacy of others may be invaded and why that risk is justified.

- **The time scale** within which data is required.

Disclosure of data

1.21 Notices under the 2016 Act will only require the disclosure of data to:
The person giving the notice i.e. the designated person; or
To another specified person who must be from the same relevant public authority. In practice, this is likely to be the single points of contact.

1.22 Where possible, this assessment will be based upon information provided by the relevant postal or telecommunications operator.

Validity of authorisations and notices.

(a) **Duration**
1.23 Authorisations and notices will only be valid for **one month**. This means the if the notice was granted on the 5 May 2014 it will expire on 4 June 2014.This period will begin when the authorisation is granted or the notice given. A designated person 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 i.e. up to one month. For 'historical' communications data disclosure may only be required of data in the possession of the postal or telecommunications operator. A postal or telecommunications operator should comply with a notice as soon as is reasonably practicable. Furthermore, they will not be required to supply data unless it is reasonably practicable to do so.
(b) **Renewal**
1.24 An authorisation or notice may be renewed at any time during the month it is valid, by following the same procedure as in obtaining a fresh authorisation or notice.

1.25 A renewed authorisation or notice takes effect at the point at which the authorisation or notice it is renewing expires.

(c) **Cancellation**
1.26 A designated person shall cancel a notice given under the Act 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 designated person who issued it.

1.27 The appropriate level of official within each public authority who may cancel a notice in the event of the designated person no longer being able to perform this duty.

1.28 As a matter of good practice, authorisations should also be cancelled in accordance with the procedure above.

1.29 In the case of a notice, the relevant postal or telecommunications operator will be informed of the cancellation. The home office provides two standard forms of cancellation notice. One form is sent to the CPS and the other is retained internally.

Retention of records by public authorities

1.30 Applications, authorisations and notices for communications data must be retained by the relevant public authority until it has been audited by the Commissioner. The public authority should also keep a record of the dates on which the authorisation or notice is started and cancelled. Records may be kept in paper, or electronic form. Facsimile copies are acceptable.

(a) ***Errors***

1.31 Where any errors have occurred in the granting of authorisations or the giving of notices, a record should be kept, and a report and explanation sent to the Commissioner as soon as is practical.

1.32 Applications must also be retained to allow for the complaints Tribunal, to carry out its functions.

1.33 The code does not affect any other statutory obligations placed on public authorities to retain data under any other enactment. (Where applicable, in England and Wales, the relevant tests given in the Criminal Procedures and Investigations Act 1996, namely whether any material gathered might undermine the case for the prosecution against the accused, or might assist the defence, should be applied).

(b) **Data protection safeguards**

1.34 Communications data, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the Data Protection Act 1998♦ and its data protection principles should be adhered to.

1.35 Data may only be disclosed to the person giving the notice or another specified person who must be from the same relevant public authority. The authorisation period of authorisations and notices is set at one month which may be renewed. A notice has to be cancelled as soon as it is clear that the reasons for which it was granted are no longer valid.

1.36 In the case of a notice, the service provider has to comply within a reasonably practicable time and only supply data if it is reasonably practicable to do so. If a CSP fails to provide the required communications data then the Secretary of State may take civil proceedings against them, which may result in the issue of, inter alia, an injunction which would have the effect of compelling the provision of data.

Introducing Data Communication evidence in court:

This evidence must be exhibited to a statement produced by the CSP. Requests for witness statements must be made via the SPOC. If it is to form the basis of questions at a formal interview under caution a statement should be obtained in advance. CSP's should be given as much notice as possible that a statement will be required. If this is considered as an after thought the evidence may not be able in the proper format when

needed and cause delays which could impinge on the statutory time limits for laying information's.

Code of Practice

1.39 The 2016 Acts provisions are subject to a statutory November 2018 code of practice. The code relates to the powers and duties conferred or imposed under IPA 2016. It provides guidance on the procedures that must be followed before access to communications data can take place under those provisions. The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Tribunal established under the Act, or to one of the Commissioners responsible for overseeing the powers conferred by the Act, it must be taken into account. The code applies to the relevant public authorities and extends to England, Wales, Scotland and Northern Ireland.

Oversight

1.41 The Act provides oversight by

The Investigatory Powers Commissioners Office (IPCO)

The Government has appointed a **Surveillance Commissioner** and his office (IPCO) to review how Public Authorities implement the requirements of RIPA. The Commissioner has wide ranging powers of access and investigation. The Council receives periodic visits from the Commissioners staff and therefore it is essential that everyone who engages in RIPA type activities is fully aware of the law and this procedure.

The Investigatory Powers Commissioner.

Lord Justice Fulford and his Judicial Commissioners are responsible for overseeing the use of investigatory powers by public authorities which include law enforcement, the intelligence agencies, prisons, local authorities and other government agencies (e.g. regulators). In total over 600 public authorities and institutions have investigatory powers.

The Commissioners are supported in this work by a body of civil servants – the Investigatory Powers Commissioner's Office (IPCO)

The more intrusive powers such as interception, equipment interference and the use of surveillance in sensitive environments will be subject to the prior approval of a Judicial Commissioner. Use of these and other surveillance powers, including the acquisition of communications data and the use of covert human intelligence sources, are also overseen by a programmed of retrospective inspection and audit by Judicial Commissioners and IPCO's inspectors.

IPCO assumed the responsibility for oversight of investigatory powers from the Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (IScomm) in September 2017. IPCO immediately takes over the inspection and audit functions of these bodies and the prior approval function of Surveillance

1.42 The Act establishes an independent Tribunal, which is made up of senior members of the legal profession or judiciary and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

Bullet points:
1.43
- An authorising officer must not only consider the communications data to be necessary for a purpose that is listed but must also consider the conduct involved in obtaining the communications data to be "proportionate to what it seeks to achieve"

- Data may only be disclosed to the person giving the notice or another specified person who must be from the same relevant public authority

- A notice has to be cancelled as soon as it is clear that the reasons for which it was granted are no longer valid.
- A central record of all authorisations/notices should be made of the above giving full details:

The type of authorisation/notice;
The date the authorisation/notice was given;
Name and rank/grade of the authorising officer;
The unique reference number (URN) of the investigation or operation;
The title of the investigation or operation, including a brief description and names of subjects, if known;
Whether the urgency provisions were used, and if so why. (Applicable to surveillance)
If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer (applicable to surveillance);
Whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice (applicable to surveillance);
The date the authorisation was cancelled.

2. RECORDING OF TELEPHONE CONVERSATIONS

The recording of telephone calls between two parties when neither party is aware of the recording cannot be undertaken, except under a Warrant granted under the 2016 Act. Such warrants are only granted by the Secretary of State and it is not envisaged that such activity would fall within the remit of local authority investigations. If it thought that such surveillance is to be undertaken, then further guidance should be sought from the RIPA Co-coordinator.

3. INTERCEPTION OF TELECOMMUNICATIONS

This power is not available to local authorities' Further advice should be sought from the RIPA Co-coordinator.

4 PROCEDURE FOR OBTAINING AUTHORISATION FOR DCS OR USE OF A CHIS

The flowcharts in Appendix 2 show the steps which are required in the authorisation procedure.

Authorising Officers (AO's)

The Regulation of Investigatory Powers Directed Surveillance and Covert Human Intelligence Order 2003 prescribes that, for Local Authorities, the Authorising Officer[3] shall be the Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent. There is no provision for officers of a lower rank to grant authorisation, even in cases of urgency.

Authorisation for DCS or use of CHIS must be given in writing by the Authorising Officer, except in urgent cases, when authorisation may be given verbally, although in such instances the procedural differences and duration of verbal authorisations, as outlined below, should be noted.

Action to be taken by the Person Applying for Authorisation.

Officers are advised to discuss the need to undertake DCS or the use of CHIS with their line manager before seeking authorisation. Options to gain the information that is required, other than by using covert techniques should be fully explored.

The Applications for Authorisation forms for DCS and CHIS operations are enclosed in Appendix 3. The forms are available to complete electronically. The person seeking authorisation should complete Parts 1 to 12 of the forms having regard to the guidance below. If the situation is urgent, verbal authorisation should be obtained from the appropriate Authorising Officer. As soon as is reasonably practicable after verbal authorisation has been given, the authorisation form should be completed, including parts 13-15 which deal with reason why the situation was considered urgent.

Following completion of Parts 1 to 12 the applying officer should obtain a unique reference number from the RIPA Coordinator[3] in Legal Services. The RIPA Coordinator will need some detail about the proposed application. It would be advisable to e-mail the form to the RIPA Coordinator. At the very least the following information will be required:

- Name of Applicant.
- Applicants department and division
- Type of Application (DCS or CHIS).
- Details of the Target of the Surveillance. (N.B. If an employee of the Council it is permissible for the full name to be withheld.)
- Whether confidential information is likely to be obtained
- Whether 'urgent provisions' are being used.

[3] The names of the appropriate Authorising Officers and RIPA Coordinator are shown in Appendix 1.

The RIPA coordinator will by return issue the URN that should be entered onto the application form before the form is submitted to the authorising Officer for consideration.

The original application as approved or refused should then be sent under cover of a sealed envelope marked for the attention of the Head of Legal and personal private and confidential. The Councils RIPA coordinator will then file the application in a secure filing cabinet after updating the Councils lists of applications and cancellations. Composite lists are held electronically by the Councils RIPA coordinator on spreadsheets for all of the Councils departments that utilize RIPA 2000 for each year from the 1st April to the 31st March.

The RIPA coordinator bearing in mind the current level of authorizations reviews and renewals will review and report back to the departments lead officer if need be.

At least annually the Councils RIPA coordinator will undertake a review of the practice and procedures undertaken by each department under RIPA and report back to each to departments lead officer.

5 GUIDANCE ON THE COMPLETION OF AUTHORISATION FORMS FOR DCS OR CHIS:

The Application for Authorisation form was previously combined to use for both DCS and CHIS Authorisations. The forms are now separate so if both a DCS and CHIS are required two forms must be completed. The latest forms are Feb 2007 and updated in September 2010 to reflect new regulations.

The revised forms are similar to the previous form save that no line manager comment need be noted. Both new forms are very similar save for 2 additional sections on the CHIS form which are dealt with at the end. The section numbers below refer to the DCS form.

Introduction

The DCS application form

This Preamble section should include the details of the officer who is requesting the authorisation and Job Number/s (if relevant) to which the investigation relates full address, contact details, operation name and operation reference number all of which should be completed.

Section 1 – Rank of authorising officer –insert job title of officer.

Section 2 – Describe the purpose of the specific authorisation or investigation

Section 3 – Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. cameras, binoculars, and recorders) that may be used.

Section 4- Details of the subject or target of the DCS should be specified. It might be necessary to state that the identity of the subject is unknown.

Section 5 – A description of the desired outcome from the surveillance. E.g. identity of the person responsible for fly-tipping.

Section 6 – Since the 5 January 2004 a local authority can only rely upon one ground of necessity for authorisation purposes i.e. for preventing or detecting crime or of preventing disorder. This should be inserted as standard on the form.

Section 7 – The section should explain why covert surveillance needs to be used and overt methods would be unsuccessful in obtaining the evidence i.e. a narrative as to why the evidence intended to be collected by the directed surveillance is necessary for the purposes of the investigation. E.g. that there are no other overt methods available to collect the information sought.

Section 8 –Details of any potential **collateral intrusion** should be specified. E.g. details of any personal information that might be collected about parties who are not the subject of the investigation. A plan should be specified as to how the potential for collateral inclusion will be minimized. E.g. by focusing line of vision on a limited area. Applicants should give as much detail as possible in this section as authorising officers will pay

particular regard to the information that is given. AO's should not authorize applications that either do not state whether collateral intrusion is likely or that do not specify what steps are to be taken to minimize it.

Section 9 – This section requires the applicant to consider whether it is proportionate to use covert methods to collect evidence. The applicant must show that the balance between the sanctity of the subjects right to privacy is outweighed by the purpose of the investigation e.g. is it the least intrusive way of obtaining the necessary evidence.

Footnotes

See OSC GUIDANCE August 2016 for definitions of necessity and proportionality

Section 10 – This section requires an indication of the likelihood of obtaining **confidential and religious information and material,** including: **matters subject to legal privilege; confidential personal information;** and **confidential journalistic information.** Such material is regarded as particularly sensitive and the likelihood of obtaining such information should be fully considered in terms of the proportionality issues that it raises. Special care should be taken when handling, retaining, copying or disseminating such information (see later – Handling of materials)

An authorisation which may involve the acquisition of confidential material may only be granted by the Head of Paid Service (Chief Executive) or in his absence his deputy.

Section11 Applicant details as set out on the form

Section 12 –Authorising officer's statement. This should state the frequency and over what period of time the covert surveillances operations will take place over the duration of the authorization i.e. until it is reviewed and cancelled.

It should be noted that a DCS authorization lasts for 3 months and a CHIS for 12 months. They can be cancelled before the end of these periods and must be cancelled in any event before the end of 3 and 12 months and must not be left to expire.

Section 13- Authorising officer's comments should deal with necessity and proportionality

The form at 9 must be considered by the authorising officer who then completes section 13 of the form with his/her own independent thought processes.

Authorising officers MUST give detailed reasons for their decision to grant authorisations.

Section 14 – If the application may involve the acquisition of confidential information or religious material the application must be considered by the Councils Chief officer as head of the Paid Service of the Council and this section completed. In such circumstances authorization should only be given in exceptional circumstances having full regard to the proportionality issues involved

Section 15 – Urgent authorisations are not permissible due to the changes made under the Protection of Freedoms Act 2012 and the need to seek approval for covert surveillance from the magistrate's court.

CHIS FORM

The CHIS form contains additional sections which must be completed

Advice should be sought from the Councils RIPA coordinator to after completing the form and before it is authorised

The applicant should sign and date the application for authorization. As mentioned above a unique reference number should be obtained from the RIPA Coordinator before submitting it to the Authorising Officer.

The form should be considered by the Authorising Officer who should complete the remaining parts of the form.

The AO should seek advice from the Councils RIPA coordinator on completion of the form

In cases where approval can only be given by the Head of Paid Service, the application should be sent to the first level Authorising Officer for initial consideration, who would then submit the form to the higher level.

CHAPTER 6 ACTION TO BE TAKEN BY THE AUTHORISING OFFICER FOR DCS OR A CHIS

Authorising officers MUST give detailed reasons for their decision to grant authorisations.

The Authorising Officer must firstly consider whether the DCS to be undertaken or CHIS to be used. Secondly, he/she must decide whether the risk of interfering with a person's private and family life, whether or not the person is the target **(collateral intrusion)** of the surveillance, is **proportionate** to the objective that is to be achieved. (See Glossary and footnotes above)

The question of proportionality and the risk of **collateral intrusion** are important considerations for the Authorising Officer to deal with. If the form does not contain sufficient information to enable an AO to consider both of these matters fully further details should be sought.

Particular consideration should be given to circumstances where confidential or religious material may be obtained. In such circumstances the application for authorisation must be considered by the Head of Paid Services his deputy.

Falls within the only ground for necessity applicable to the Council i.e. for the purpose of preventing or detecting crime or of preventing disorder. Whist there is no definition of what this means it is likely to be given a wide definition by the courts.

The Authorising Officer must complete those parts of the application for authorisation and make a decision as to whether to approve or refuse the application. Only in circumstances where verbal authorisation has been given previously is it necessary to complete those parts of the DCS form.

If evidence collected by way of DCS is challenged in the Court, it will help the Council's case if the AO has recorded in some detail his/her comments as to why the authorization was granted. In particular, the AO's comments on necessity, proportionality and collateral intrusion should be thorough. An AO must also state precisely what activity is authorized bearing in mind that an applicant might seek authority for a variety of activities, not all of which might be granted.

Both forms require the Authorising Officer to specify a date when the authorization should be reviewed and the frequency of review thereafter. In most typical authorizations it is likely that only one review (if any) will be required. A review form has to be completed (see Appendix 3) to record any review that does take place.

If approved, the authorisation lasts for three months in the case of DCS authorisations, and twelve months for CHIS authorisations. Both must be cancelled and not left to expire

If the application may involve the acquisition of confidential or religious material the application must be considered by the Chief Executive or his deputy, who then becomes the Authorising Officer.

An additional Section must also be completed to confirm that the issue of religious and confidential material has specifically been taken into account. In such circumstances authorisation should only be given in exceptional and compelling circumstances having full regard to the proportionality issues involved.

The original of the completed authorisation form, whether approved or refused, should be sent to the RIPA Coordinator.

A copy of the form should be retained by the Authorising Officer and a further copy returned to the Applicant for retention on the investigation file.

CHAPTER 7 DURATION OF AUTHORISATIONS RENEWALS AND CANCELLATIONS FOR DCS AND CHIS

DCS authorisations will cease to have effect three months from the date of approval and CHIS authorisations, twelve months from the date approval. They must be cancelled before the expiry of the 3 and 12 months' periods.

Urgent verbal authorisations will cease to have effect after 72 hours, beginning with the time when the authorisation was granted, unless subsequently endorsed by written authorisation.

It will be the responsibility of the officer in charge of an investigation to ensure that any DCS or use of CHIS is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect. The RIPA co-coordinator shall also perform a monitoring role in this respect **but the primary responsibility rests with the Officer in charge.**

Renewals

An Authorising Officer may renew an authorisation before it would cease to have effect if it is necessary for the authorisation to continue for the purpose for which it was given. Such renewals would normally extend the authorisation period for a further three months beginning with the day on which initial authorisation would cease to have effect, but for the renewal. Authorisation may be granted more than once, provided they continue to meet the criteria for authorisation. An application for renewal must not be made more than seven days before the authorisation is due to expire.

The officer requesting the renewal should complete Parts 1 to 6 of the Application to Renew a DCS or CHIS Authorisation form (Appendix 3) and submit this to the Authorising Officer for consideration and completion of Part 7 and 8. The Authorising Officer must consider the application for renewal in relation to the original purpose for which authorisation was granted, taking into account any change in circumstances.

If the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then the outstanding authorisation should be cancelled and new authorisation sought.

All completed **original** renewal forms must be immediately sent to the RIPA Coordinator. A copy of the form should be retained by the Authorising Officer and a further copy sent to the Applicant for retention on the investigation file.

Cancellations

All authorisations, including renewals, must be cancelled if the reason why DCS or use of CHIS was required no longer exists. This will occur in most instances when the purpose for which surveillance was required has been achieved and officers must be mindful of the need to cancel any authorisation which has been issued. The responsibility to ensure that authorisations are cancelled rests with the Officer in charge.

To cancel an authorisation, the person in charge of the investigation to which the authorisation relates should complete parts 1 to 4 of the Cancellation of Authorisation

form (Appendix 3). The form should be submitted to the Authorising Officer for endorsement and completion of Part 5.

All completed **original** cancellation forms must be sent to the RIPA Coordinator. A copy of the form should be retained by the Authorising Officer and a further copy sent to the Applicant for retention on the investigation file.

8 HANDLING MATERIAL OBTAINED FROM DCS AND CHIS OPERATIONS

Material, or product, such as: written records (including notebook records); video and audio tape; photographs and negatives; and electronic files, obtained under authorisation for DCS or CHIS operations should be handled, stored and disseminated according to the following guidance.

Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with the established disclosure requirements having regard to the Criminal Procedure and Investigations Act 1996 and Civil Procedure Rules. Further guidance on this can be obtained from the RIPA Co-coordinator.

Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

Material may be used in investigations other than the one which authorisation was issued for. However, use of such material outside the Local Authority, or the Courts, should only be considered in exceptional circumstances.

Where material obtained is of a confidential nature then the following additional precautions should be taken:

- Confidential material should not be retained or copied unless it is necessary for a specified purpose.

- Confidential material should only be disseminated, on legal advice, that it is necessary to do so for a specific purpose.

- Confidential material that is retained should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person who might prejudice any civil or criminal proceedings.

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

If in doubt about what constitutes confidential material and the handling etc. of such material, then advice should be sought from the appropriate RIPA Codes of Practice or from the RIPA co-coordinator.

9 THE ROLE OF THE RIPA CO-ORDINATOR FOR DCS AND CHIS APPLICATIONS

The Council RIPA coordinator is responsible for **raising RIPA awareness** across the Council as a whole The Coordinator should periodically publish brief guidance in the Councils internal newsletter e.g. Pride at Work and on the Council intranet

All applications for authorisation (including those that have been refused), renewals and cancellations will be retained for a period of at least five years by the RIPA Co-coordinator.

In addition to the above the RIPA Co-coordinator shall: -

Keep a record (see Appendix 5) of all applications for authorisations whether finally granted or refused.

Allocate to each application a unique reference number.

Maintain a system for the purpose of identifying and monitoring expiry dates and renewal dates although the responsibility for this is primarily that of the Officer in charge.

Consider all authorisations for the purpose of monitoring types of activities being authorised to ensure consistency and quality throughout the Council.

Assist all departments in identifying and fulfilling training needs. Most investigatory departments should by now have received some training although training should be seen as an ongoing exercise.

The periodic review of this procedure document.

Assist council staff to keep abreast of RIPA developments.

Carry out a periodic quality control exercise and inform relevant parties of the findings of the exercise.

10 GLOSSARY OF TERMS

Surveillance

Includes:

- 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 surveillance;
- surveillance by or with the assistance of a surveillance device; and
- The interception of a communication in the course of its transmission by means of a postal service or telecommunication system if it is one sent by, or intended for, a person who has consented to the interception of the communication.

But does not include:

- the conduct of a covert human intelligence source in obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source;
- general targeting of a problem area, or covert observation of a premises which does not involve systematic surveillance of an individual, even where such observation may involve the use of equipment which reinforces normal sensory perception, such as binoculars or cameras.
- The general use of CCTV systems, because the public are aware of their use, i.e. they are overt.

Covert Surveillance

Means surveillance which is carried out in a manner calculated to ensure that the person's subject to the surveillance are unaware that it is or may be taking place.

Covert Relationships (CHIS)

Means a relationship conducted in a manner calculated to ensure that one or more of the parties to the relationship Is unaware of its purpose.

Communications	This is data about communications. It relates to data generated or acquired by the SP in delivering / fulfilling services to its customers. Local Authorities are not entitled to access this information. The information includes: Information identifying the sender and recipient (including copy recipients) of a communication. Routing information identifying or selecting any apparatus, such as equipment, machinery or device, or any wire or cable) through which a communication is transmitted e.g. dynamic IP address allocation, web postings and email headers (to the extent that the content of the communication is not disclosed-the subject line of an email is considered content) Information identifying any location of a communication, such as mobile phone cell site location. Call detail records for specific phone calls i.e. Call Line Identity (CLI) Web browsing information (to the extent that only the host machine or domain name (website name) is disclosed. Information written on the outside of a postal item. Online tracking of communications (including postal items)
Service data	This relates to the use of the SP's services by Customers, and includes: - The periods during which the customer used the service(s) Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers 'Activity', including itemised records of telephone calls (numbers calls) internet connections, dates and times/duration of calls, text messages sent

	Information about the connection, disconnection and reconnection of services Information about the provisions of conference calling, call messaging, call waiting and call baring telecommunications services Records of postal items such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection Top up details for pre-pay mobile phones –credit/debit card voucher /e-top up details
Customer Data	Customer data is the most basic. It is data about users Of communications services. This data includes: - Name of the customer – subscriber information (known as 'subscriber checks' or 'reverse hook up' and includes subscribers of email accounts and or web space.
Surveillance Device	Means any apparatus designed or adapted for use in surveillance.
Residential Premises	Means any **premises** occupied by any person, however temporarily, for residential purposes or other wise as living accommodation (including hotel or prison accommodation), but does not include common areas to such premises. **Premises** also include any vehicle or moveable structure used within the definition above.
Proportionate	Whether it is proportionate to use covert methods to collect evidence. You must show that the balance between the sanctity of the subject's right to privacy is outweighed by the purpose of the investigation. E.g. is it the least intrusive way of obtaining the necessary evidence.

Footnotes

See OSC GUIDANCE July 2016 below for further guidance and 2018 Codes of Practice

Necessity
And Proportionality

Private Vehicle	Means any **vehicle** which is used primarily for private purposes of the person who owns it or otherwise has a right to use it, but would not include any person whose right to use the vehicle arises from making payment for a particular journey. **Vehicle** also includes any vessel aircraft or hovercraft.
Private Information	Includes any information relating to a **person**'s private or family life. Private life also includes activities of a professional or business nature (Amann v Switzerland (2000) 30 ECHR 843). "**Person**" also includes any organisation and any association or combination of persons.
Immediate Response	Includes a response to circumstances or events which, by their very nature, could not have been foreseen.
Collateral Intrusion	Includes situations where there is a risk of the surveillance resulting in private information being obtained about persons other than the subject of the surveillance.
Confidential Material	Includes: ▪ **matters subject to legal privilege;** ▪ **confidential personal information**; or ▪ **Confidential journalistic material**.
Matters Subject to Legal Privilege	Includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege.
Confidential Personal Information	Includes information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating: ▪ to his/her physical or mental health; or ▪ to spiritual counselling or other assistance given or to be given, and ▪ which a person has acquired or created in the course of any trade, business, profession or other occupation, or for

the purposes of any paid or unpaid office.

It includes both oral and written information and also communications as a result of which personal information is acquired or created. 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 secrecy contained in existing or future legislation.

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. This 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.

PART TWO – INTERPRETATIONAL GUIDANCE

Each activity should be considered on its merits

67. It is unacceptable to consider whether an authorisation is required based on the description of the surveillance. Test purchase operations conducted by law enforcement agencies (e.g. in drugs operations) are significantly different from those normally conducted by local authorities (e.g. by Trading Standards). “Drive-by” surveillance may or may not require an authorisation depending on the circumstances.

68. The application of the legal principles of covert surveillance to particular facts is, ultimately, a matter of judgment: the extent to which judgment can be prescribed is limited; there cannot be a one-size-fits-all catalogue of principles, and it would be misleading if Authorising Officers, in particular, were to believe that such a chimera exists.

69. A common error when considering whether authorisation is required is to restrict contemplation to the type of tactic rather than the specific facts of the activity. It is unwise to approach RIPA or RIP(S)A form the perspective of labels.

The effect of section 80 RIPA and section 30 RIP(S)A

70. Part I of RIPA makes unauthorised interception unlawful. In contrast, Part II makes authorised surveillance lawful but does not make unauthorised surveillance unlawful. Whilst not an obligation there is an expectation that Part II covert surveillance is authorised. Section 80 RIPA and section 30 RIP(S)A help a trial judge in exercising his discretion regarding the admissibility of evidence and the impact of the way that evidence was obtained on the fairness of a trial. It is inappropriate to cite these sections as justification for a decision not to authorise. It is unwise for a public authority to rely on them as protection from liability if it chooses not to authorise covert surveillance. It is one of the functions of the Office of Surveillance Commissioners to prevent abuse of discretionary powers.

The roles of the applicant and the Authorising Officer are different

71. The role of the applicant is to present the facts of the application for covert surveillance: the crime to be investigated; the reason why it is proposed to conduct the investigation covertly; what covert tactics are requested and why; whom the covert surveillance will be focused on; who else may be affected by it and how it is intended to conduct covert surveillance. To assist the Authorising Officer’s assessment of proportionality, the applicant should provide facts and evidence but it is not the role of the applicant to establish that it is necessary and proportionate; that is the statutory responsibility of the Authorising Officer.
[21]

Necessity
72. The Authorising Officer must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in section 28(3) of RIPA and section 29(3) of RIP(S)A. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. Often missed is an explanation of why it is necessary to use the covert techniques requested.

Proportionality
73. Proportionality is a key concept of RIPA and RIP(S)A. It is often poorly articulated. An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

74. A potential model answer would make clear that the following elements of proportionality had been fully considered:

74.1 balancing the size and scope of the operation against the gravity and extent of the perceived mischief
74.2 explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
74.3 that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
74.4 providing evidence of other methods considered and why they were not implemented.
"I am satisfied" and "I believe"
75. The Authorising Officer should set out, in his own words, why he is satisfied (RIP(S)A) or why he believes (RIPA) the activity is necessary and proportionate. A bare assertion is insufficient.
[22]

An Authorising Officer must demonstrate his satisfaction with the intelligence on which an application is made

76. To assist an Authorising Officer to reach a proper judgment, the value of the data, information or intelligence on which the application has been made should be clear. It is considered best practice for law enforcement agencies to utilise standard evaluation nomenclature which grades both the source and the information. While it is not necessary or desirable in the application to spell out in detail the content of intelligence logs, cross-referencing to these enables an Authorising Officer to check detail. Particular care should be taken when using data or information obtained from open or unevaluated sources such as the Internet or social networks.

77. The law prevents an applicant or Authorising Officer from referring to interception and this presents significant difficulty when covert surveillance is to be based solely on that type of intelligence. Without product derived from other acquisition methods, or an approved summary of the closed material, covert surveillance cannot be authorised.

The impact of UK Statutory Instrument 2010/521 and 2012/1500 (restricting local authority grounds under section 28(3)(b) of RIPA)

78. Local authorities in England and Wales can no longer seek the protection of the Act on the grounds provided by subsections 28(3)(d) and (e) (i.e. in the interests of public safety and for the purpose of protecting public health). In relation to directed surveillance (though not to authorising CHIS), their remaining powers were further limited by Statutory Instrument 2012/1500. To authorise directed surveillance, the Authorising Officer must demonstrate that the proposed activity is necessary for the prevention or detection of a crime which either carries a maximum sentence of at least six months' imprisonment or is an offence relating to the sale of alcohol or tobacco products to minors. (As to the definition of "detecting crime", see RIPA section 81(5).)

All covert activity that is not properly authorised should be reported as soon as it is recognised

79. Activity which should properly be authorised but which isn't should be reported to the Chief Surveillance Commissioner, in writing, as soon as the error is recognised. An initial e-mail alerting the OSC should be followed by a report detailing the circumstances and remedial action submitted by the Chief Officer or Senior Responsible Officer. This does not apply to covert activity which is deliberately not authorised because an Authorising Officer considers that it does not meet the legislative criteria, but allows it to continue. It does include activity which should have been authorised but wasn't or which was conducted outwith the directions provided by an Authorising Officer. All activity which should have been authorised but was not should be recorded and reported to the Inspector(s) at the commencement of an inspection to confirm that any direction provided by the Chief Surveillance Commissioner has been followed.
[23]

80. When it is decided to use covert surveillance without the protection of RIPA or RIP(S)A it would be prudent to maintain an auditable record of decisions and actions. Such activity should be regularly reviewed by the Senior Responsible Officer.

The effect of the Policing and Crime Act 2009

81. The Policing and Crime Act 2009 amends section 93 PA97 and sections 29 and 33 of RIPA. It enables law enforcement agencies to enter into written collaborative agreements regarding the provision of support within the operating area of the relevant collaborative units. For a collaboration agreement to take effect, the terms of the agreement must explicitly permit officers of the prescribed rank, grade or office to make applications or authorisations or to have day-to-day responsibility for dealing with a CHIS or to have general oversight of the use made of a CHIS or to have responsibility for maintaining a record of the use made of a CHIS or to be used as a CHIS. The CHIS Code of Practice paragraphs 6.10 to 6.13 provide for the authorised control and handling of a CHIS who benefits more than one authority. The Covert Surveillance and Property Interference Code of Practice paragraphs 3.20 to 3.22 provide for applications and authorisations for directed and intrusive surveillance and property interference where there is a collaboration agreement.

82. If there is no written collaboration agreement, the arrangements provided at paragraphs 7.12 to 7.13 of the Covert Surveillance and Property Interference Code of Practice and paragraph 5.9 of the CHIS Code of Practice must be followed.

Related Authorisations

83. If the action authorised refers to activity under a previous authorisation, the Unique Reference Number (URN) and details of that authorisation (e.g. details of a vehicle which has a VTD fitted) should be given to enable the Commissioner to cross-refer. The Authorising Officer should ensure that what is being granted is not in conflict with previous or other current authorisations. Careful attention must be paid to the relationship between property interference and directed surveillance authorisations to ensure that the subsequent download, interrogation or use of the product from the property interference is clearly spelt out on the associated directed surveillance authorisation. Similarly, authorisations for directed surveillance should only permit the download, interrogation or use of product from interference on the condition that a valid PA97 authorisation exists.
[24]

The Authorising Officer must state explicitly what is being authorised
84. Sections 28(4)(a) and 32(5) of RIPA require the Authorising Officer to describe and specify what he is granting. This may or may not be the same as requested by the applicant. For the benefit of those operating under the terms of an authorisation, or any person who may subsequently review or inspect an authorisation, it is essential to produce, with clarity, a description of that which is being authorised (i.e. who, what, where, when and how). The Authorising Officer should as a matter of routine state explicitly and in his own words what is being authorised, and against which subjects, property or location. Mere reference to the terms of the application is inadequate.

Authorisation different from application
85. If an application fails to include an element in the proposed activity which in the opinion of the Authorising Officer should have been included (for example, the return of something to the place from which it is to be taken for some specified activity), or which is subsequently requested orally by the applicant, it may be included in the authorisation; if so, a note should be added explaining why. Conversely, if an Authorising Officer does not authorise all that was requested, a note should be added explaining why. This requirement applies equally to intrusive surveillance, property interference, directed surveillance and CHIS authorisations.

Careful use of words
86. The Authorising Officer must be careful in the use of “or” and “and” in order not to restrict what is intended. For example, do not use “or” when “and” is meant (e.g. “deployment of …. on vehicle A or vehicle B” limits deployment to either vehicle, not both simultaneously or one after the other).
[25]

Duration of authorisations and renewals

87. Every authorisation must be for the statutory period, normally three months for surveillance authorisations and twelve months for CHIS authorisations. Thus a surveillance authorisation granted at 14:10 hrs on 9 June will expire at midnight on 8 September. To avoid any risk of ambiguity, this should be expressed as 23:59 hrs on 8 September. If that authorisation is subsequently renewed for a further statutory period, then as with a motor insurance policy, the renewal will begin, using the preceding example, at 00:00 hrs on 9 September, expiring at 23:59 hrs on 8 December, with any subsequent renewal starting at 00:00 hrs on 9 December, and so on. Where longstanding electronic systems or adopted processes show the renewals beginning at 23:59 hrs, thus "losing a day" at each subsequent renewal, OSC Inspectors shall not criticise this, nor consider it a breach. Urgent oral authorisations last for 72 hours (though see Note 295 regarding local authorities in England & Wales). Authorisations for juvenile CHIS last for one month, and for those likely to acquire legally privileged material, three months (with a Surveillance Commissioner's prior approval). For all authorisations the time period begins when an authorisation is granted, unless the prior approval of a Commissioner is required, or a magistrate must first approve the activity (under The Protection of Freedoms Act 2012). In the former, the period begins when written notice of the Commissioner's approval is received by the Authorising Officer. In the latter, upon the date and time the authorisation is approved by the magistrate. The fact that the operation to which the authorisation relates is only expected to last for a short time cannot affect the authorisation period. An early review can take care of issues of continuing necessity and proportionality.

Renewals

88. Renewals can only be granted before the expiry of the existing authorisation and take effect from the time of that expiry. This applies equally to renewals requiring a Commissioner's prior approval, provided that the Authorising Officer has received written notice of that approval before that time.

Dates of effectiveness - leaving date boxes blank

89. Because authorisations requiring prior approval will only be effective on receipt by the Authorising Officer of written notice of the Commissioner's approval, the date boxes should be left blank until the decision has been received. If, for any reason, the Authorising Officer does not personally see a Commissioner's prior approval (for example, when a Chief Constable is out of the force area), receipt in the office of the Authorising Officer will suffice, as an indication of the Authorising Officer having received written notice of approval. See paragraph 6.11 of the Covert Surveillance and Property Interference Code of Practice. The Commissioners require forces which adopt this procedure to notify the Authorising Officer, by an effective and auditable means, of any comments by the Commissioner when giving approval. [26]

Dates of effectiveness - renewal information required by the OSC
90. The OSC must be notified of the effective to and from dates when the authorisation is renewed. Where a renewal requires a Commissioner's prior approval, the dates of effectiveness should be accompanied by a note from the Authorising Officer acknowledging that the dates are conditional upon receipt of approval before the expiry of the current authorisation.

The rank of the Authorising Officer should be provided
91. Every authorisation should show the rank of the person giving it. Designated Deputies must identify themselves as such and say why they are giving the authorisation. ACCs who are not Designated Deputies should state when it would next be reasonably practicable for the Authorising Officer or Designated Deputy to consider the application. Where a new Chief Constable or Designated Deputy is appointed, the OSC should be notified as soon as possible.

Renewals involving minor changes
92. Commissioners are content to treat as renewals authorisations where minor changes have occurred, e.g. the removal of a person or a vehicle from the investigation or the addition to the authorisation of previously unknown details such as a vehicle registration or a subject's identity, provided that the terms of the original authorisation allowed for such amendment. Where details in authorisations are amended at renewal, the reason for further identification or removing subjects or vehicles must be given.

Persons, groups, associates, and vehicles
93. Subject to the guidance at Note 99, reviews and renewals should not broaden the scope of the investigation but can reduce its terms. Where other subjects may unexpectedly come under surveillance, and provided it is justified by intelligence, authorisations can anticipate it by using words such as "suspected of", "believed to be" or "this authorisation is intended to include conversations between any and all of the subjects of this investigation, including those whose identities are not yet known but are believed to be involved in the criminality". When the identities of the other criminal associates and vehicle details become known, they should be identified at review and in the renewal authorisation, so long as this is consistent with the terms of the original authorisation. Otherwise, fresh authorisations are required.

94. When an authorisation includes a phrase such as "...other criminal associates..." a review or renewal can only include those associates who are acting in concert with a named subject within the authorisation (a direct associate) and who are believed to be engaged in crime. It does not enable "associates of associates" to be included, for whom a fresh authorisation is required.
[27]

95. Where a person or a vehicle can be identified they must be. If, for example, a subject drives two known vehicles but has access to others and the property interference or covert surveillance may take place on or in any of the vehicles, the wording of the authorisation must reflect this and the two known vehicles be specified in the authorisation, as well as a suitable formula to allow for deployment on as yet unidentified vehicles.

96. It is acceptable to authorise surveillance or property interference against a group or entity involving more than one individual (for example an organised criminal group where only some identities are known) providing that it is possible to link individuals to the common criminal purpose being investigated. It is essential to make explicit the reasons why it is necessary and proportionate to include persons, vehicles or other details that are unknown at the time of authorisation, but once identified they should be added at review (see Note 100). The Authorising Officer should guide the operational commander by setting contextual parameters for the use of the “link” approach.

97. The Authorising Officer should be updated when it is planned to deploy equipment or surveillance against a freshly identified subject before such deployment is made, to enable him to consider whether this is within the terms of his original authorisation, necessary, proportionate and that any collateral intrusion (or interference) has been taken into account; alternatively, where operational demands make it impracticable for the Authorising Officer to be updated immediately, as soon as reasonably practicable thereafter. This is to ensure that the decision to deploy further devices or surveillance remains with the Authorising Officer and is not delegated to, or assumed by, another, such as the operational commander. Such reviews should be pertinent and can be done outwith the usual formal monthly written review process, provided that the details of the Authorising Officer’s decisions are recorded contemporaneously and formally updated at the next due review. Where the terms of an authorisation do not extend to interference to other subjects (criminal associates) or their property then a fresh authorisation, using the urgency provisions if necessary, will need to be sought.

98. It is no longer necessary to notify the OSC in writing of the identification of any vehicle, property or person that could not be identified at the time authorisation was given. However, it is vital that details are recorded at the next review or renewal. It is wise to confirm in writing, at cancellation, the details of all property interfered with and all people’s subject to surveillance, where these have been identified.

(See also Note 110) [28]

Directed surveillance tactics and techniques may be amended
99. This note applies to directed surveillance only; existing procedures for new interference with property or new methods of intrusive surveillance remain. To comply with *R v Sutherland,* the Authorising Officer should clearly set out what activity and surveillance equipment is authorised in order that those conducting the surveillance are clear on what has been sanctioned at each stage in the authorisation process. It is recognised that it is not always possible, at the outset of an investigation, to foresee how it will progress, but this should not provide a reason for applicants to request a wide number of tactics "just in case" they are later needed. The Authorising Officer may not authorise more than can be justified at the time of their decision and should demonstrate control and a proper understanding of necessity, collateral intrusion and proportionality, relating to each tactic requested. In straightforward cases, an applicant should request only the tactics that are known to be available and intended to be used. In more complex cases, where it is foreseen based on operational experience and assessed intelligence that additional tactics may be required as the investigation develops, additional tactics may be requested by way of review. The Authorising Officer should consider the use made of tactics to date, along with their impact and any product, to ensure that each additional tactic is necessary, whether collateral intrusion can be justified, and whether the cumulative effect of the tactics is proportionate in light of progress. Amendment must be explicit and no tactic may be used prior to it being granted by an Authorising Officer. OSC inspections will place significant emphasis on review and renewal procedures to ensure that Authorising Officers are addressing legal requirements throughout the life of an authorisation.

100. Authorisations against a named subject should indicate when, where, and in what circumstances the surveillance is to be carried out.

What must be specified in authorisations (section 32(5) of RIPA and section 6(5) of RIP(S)A)
101. Intrusive Surveillance authorisations must specify or describe (a) the type of surveillance, (b) the premises or private vehicle, and (c) the investigation or operation. For example, an authorisation for the use of an audio device could be for "the monitoring and recording of conversations taking place between X and Y at Z address in connection with operation W, an investigation into drug trafficking".

Crime other than specified in authorisation
102. Discussion by subjects of crimes other than such as are specified in an authorisation need not be disregarded.
[29]

Interference when there is no serious crime
103. Interference of this type cannot have the protection of PA97 but it is not unlawful in itself. It is sometimes necessary and proportionate to interfere with property in order to locate a missing person or where there is a perceived threat to life not in relation to criminal conduct or where it is necessary for training purposes. However, it is capable of giving rise to a breach of privacy (e.g. some missing persons may not wish to be located) and law enforcement agencies should have in place a policy and procedure for the use of specialist equipment in these circumstances which should include an audit of the activity sanctioned. There is no requirement to inform the OSC when equipment is used for these purposes but agencies should bring such instances to the attention of the OSC Inspector during the next inspection.

Absence of Authorising Officer (section 94(1) of PA97, section 34(2) of RIPA and section 12(2) of RIP(S)A)
104. It is unlikely to be regarded as "not reasonably practicable" (within the meaning of sections of the Acts specified above) for an Authorising Officer to consider an application, unless he is too ill to give attention, on annual leave, is absent from his office and his home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not to be regarded as rendering it impracticable for an Authorising Officer to consider an application. Where a deputy for a Force Authorising Officer acts in his stead, this should be on a substantive basis as a Superintendent (or equivalent), and not a temporary or convenient arrangement purely for the duration of the consideration of an authorisation in their absence or to cope with reduced headcount.

105. Where a Designated Deputy gives an authorisation the reason for the absence of the Authorising Officer should be stated.

Authorisations under section 93(3) of PA97: execution by another organisation
106. The absence of a collaboration agreement does not preclude the application seeking authorisation of actions by members of another organisation. This guidance is extended to RIPA and RIP(S)A.

(See also Note 112)
Cancel at the earliest opportunity
107. If, during the currency of an authorisation, the Authorising Officer is satisfied that the authorisation is no longer necessary, he must cancel it. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. In the case of authorisations for property interference and intrusive surveillance, the Authorising Officer should, within four working hours of signing the cancellation, give notice to a Commissioner (which in practice means the OSC) that he has done so.
[30]

108. Where interference with more than one property is authorised on a single authorisation (see Note 161) cancellation of individual items may be effected by way of review. The Authorising Officer should fulfil the requirement set out in Note 110. When the interference with all property has ceased a cancellation should be submitted which clarifies which property was interfered with and the duration of each interference.

109. Authorisations may be cancelled orally. When and by whom this was done should be endorsed on the cancellation form when it is completed, and recorded on the Central Record of authorisations.

(See also Part 1, Note 33)

Cancellation – information required

110. Although paragraph 5.18 of the Covert Surveillance and Property Interference Code of Practice is correct in saying that there is no *requirement* for any further details to be recorded when cancelling a directed surveillance authorisation, the Commissioners consider that it would be sensible to complete the authorisation process in a form similar to other parts of the authorisation where relevant details can be retained together. When cancelling an authorisation, the Authorising Officer should:

110.1 Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.
110.2 The reason for cancellation.
110.3 Ensure that surveillance equipment has been removed and returned.
110.4 Provide directions for the management of the product.
110.5 Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.
110.6 Record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

The use by one authority of another to conduct surveillance for a crime that it has no capability to prosecute

111. RIPA and RIP(S)A deal not with enforcement powers but the acquisition of information; there is no obligation to do something with the information collected. It is acceptable for one authority to use the services of another even if the requesting authority has no power or intent to use the product providing that the surveillance is necessary and proportionate to what it seeks to achieve. CHIS should not be exposed to unnecessary risk to obtain information that is unlikely to be used.
[31]

The use of external partners
112. When a person who is not an employee of the public authority is authorised to conduct covert surveillance, he is an agent of the public authority. This applies to private contractors or members of another public authority. It is unwise to assume competence and, where there is doubt, an Authorising Officer should check it and record that he has done so. It is wise, if no collaboration agreement exists, to obtain written acknowledgement that they are an agent of the public authority and will comply with the authorisation. Third parties authorised by a public authority are liable to inspection by the Office of Surveillance Commissioners regarding their conduct in relation to the activity authorised.

Disclosure of techniques
113. A Surveillance Commissioner and an Authorising Officer can only authorise on the basis of what has been provided in writing. Issues of disclosure should not inhibit the proper construction of applications and authorisations but can be dealt with at the appropriate time using existing procedures.

One public authority may not force the terms of an authorisation on another
114. One authority may request another to conduct covert surveillance on its behalf (see Note 106) but it may not force those conducting the surveillance to act in a manner that is counter to their beliefs or where the risk is unacceptable to them. If agreement cannot be reached, then the requesting authority will have to find an alternative solution.

Requests to amend data
115. If an overt approach is made to the owner of data to amend data that he holds to prevent the compromise of a covert investigation (for example, amendment to flight manifests or delivery tracking details), property interference authorisation is not necessary. It would be prudent, however, for the request and amendments to be made in an auditable manner so that the data owner is appropriately protected. [32]

The retention of applications with 'wet signatures'
116. The key signature is that of the Authorising Officer on the authorisation. The only way it is possible to establish that the Authorising Officer has applied his own mind to the authorisation is if it is handwritten by him. Typed documents are open to the suggestion that the authorisation is prepared by another and simply signed by the Authorising Officer. If information technology is used to construct applications and authorisations, it must be capable of authenticating the author of each version. In the absence of authentication, hand-written (so-called 'wet') signatures are required to avoid accusation that the authorisation has been altered *ex post facto*. If an Authorising Officer relies on words prepared by another, his signature signifies responsibility for those words. Authorisations with wet signatures may be retained by the Authorising Officer or centrally, the latter being the preferred option. It is always open to a trial judge to require evidence which satisfies him that documents relied on are authentic. All public authorities must be ready to provide the relevant witness where authenticity is open to question.

The meaning of Professional Legal Adviser
117. Legal privilege attaches to communications with a legal adviser (usually involving a contractual relationship). It would not normally apply to a Trade Union representative but would normally apply to a Barrister, Solicitor, Legal Executive or Solicitor’s Clerk.

The design of forms
118. The Commissioners will continue to criticise the use of forms which do not require the Authorising Officer to fulfil his or her statutory responsibilities. Forms should enable authors to comply with legislation which requires an Authorising Officer to explain the details required by the legislation (see also Notes 75 and 84). There are benefits to the adoption of a common design, but a public authority may amend forms if it encourages precision. The use of pre-scripted assertions is usually inadequate.

Combined authorisations
119. Although an authorisation combining one or more types of covert activity is within the legislation, such contribution often causes error; for example, directed surveillance can only be authorised for three months and a CHIS may only be authorised for 12 months and ensuring synchronised documentation is difficult. It should also be remembered that property interference and intrusive surveillance require separate authorisations because they are made under different Acts. (See also Note 161).
[33]

Retention of property
120. The principles of RIPA regarding the retention of property apply equally to PA97 (see Covert Surveillance and Property Interference Code of Practice paragraphs 1.2, 9.4 to 9.6 and 7.33 to 7.34).

The Authorising Officer should fully understand the capability of surveillance equipment
121. In order to give proper consideration to collateral intrusion, and to comply with *R v Sutherland,* the Authorising Officer must fully understand the capabilities and sensitivity levels of technical equipment intended to be used, and where and how it is to be deployed. An application which does not assist the Authorising Officer in this respect should be returned for clarification (see also Note 284).

122. The Commissioners are aware that some specialist equipment extracts automatically more data than can be justified as necessary or proportionate and may give rise to collateral intrusion. The inability of technology to restrict capability should not dictate the terms of an authorisation. If data is obtained that exceeds the parameters of an authorisation, the Authorising Officer should immediately review it and make arrangements for its disposal.

Those required to respond to tasking should see the authorisation
123. Where Technical Surveillance Units or other officers are required to respond to tasking, they should see a copy of the authorisation and of any comments by a Surveillance Commissioner or Authorising Officer. For directed surveillance not involving the installation of devices, it is sufficient for the officer in charge of the surveillance team to see these documents and then to brief the team accordingly while taking care to repeat precisely the form of words used by the Authorising Officer. In the case of CHIS, the handler should not proceed until the authorisation has been seen. In each case there should be acknowledgement in writing (with date and time) that the authorisation has been seen.

Private information - activity in public
124. Section 26(2) RIPA does not differentiate between current and historical surveillance product. Sections 48(2) of RIPA and section 31(2) of RIP(S)A define surveillance as including “monitoring, observing or listening” which all denote present activity; but present monitoring could be of past events or the collation of previously unconnected data. Pending judicial decision on this difficult point the Commissioners’ tentative view is that if there is a systematic trawl through recorded data (sometimes referred to as “data-mining”) of the movements or details of a particular individual with a view to establishing, for example, a lifestyle pattern or relationships, it is processing personal data and therefore capable of being directed surveillance. [34]

125. The checking of CCTV cameras or databases simply to establish events leading to an incident or crime is not usually directed surveillance; nor is general analysis of data by intelligence staff for predictive purposes (e.g. identifying crime hotspots or analysing trends or identifying criminal associations). But research or analysis which is part of focused monitoring or analysis of an individual or group of individuals is capable of being directed surveillance and authorisation may be considered appropriate.

(Covert Surveillance and Property Interference Code of Practice 2.6 refers.)

The "Kinloch" judgment (Kinloch v Her Majesty's Advocate [2012] UKSC 62)

126. It is fundamental to all authorisations that they are granted *before* any activity takes place, and thus, before anyone can tell what will happen or has happened. The whole process of authorising covert activity, including what is said at paragraph 1.14 of the Covert Surveillance and Property Interference Code of Practice, is based upon what may happen in terms of likelihood. Put another way, the need for an authorisation has to be judged at the time of authorisation, not with the benefit of hindsight. This principle is crucial when considering the implications of *Kinloch*, where there had been no authorisation but the Supreme Court knew and gave judgment about what had actually happened.

127. The Supreme Court stressed, in paragraph 18 of its judgment, the Strasbourg jurisprudence that "whether there has been an interference with the right to respect for a person's private life.....will depend in each case on its own facts and circumstances". It is of significance that (1) the Court was not considering whether an authorisation for directed surveillance ought to have been granted, nor addressing issues of collateral intrusion or proportionality; and (2) the Court nowhere said or implied that activity in a public place is, if covertly observed by agents of the state, immune from the need for a directed surveillance authorisation.

Biographical information does not satisfy the private information test on its own

128. Use of the term "biographical information" appears to have resulted from the data protection case of *Durant v Financial Services Authority [2003] EWCA Cave 1746*. The Court of Appeal was construing the Data Protection Act 1998, which gave effect to the EC Directive in relation to the protection of personal data and its holding by data controllers. In construing the meaning of "personal data" in section1(1) of the Act, the Court held that one of the two notions which may be of assistance is "whether the information is biographical in a significant sense, that is going beyond the recording of the protective data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy would not be said to be compromised". It is important to note about this decision that:

[35]

127.1 Section 1(1) defines “personal data” by reference to individuals who can be identified from data: it is therefore obvious that “personal data” is a different concept from private information
127.2 It was not concerned with RIPA nor was the Court referred to the Strasbourg decisions in relation to private or family life
127.3 “Private information” in RIPA section 26(10) reflects private life in Article 8. “Private life” has been broadly defined at Strasbourg to include professional and business activities.
129. It is dangerously misleading to seek to apply a court’s tests for construing a term in one statute to the construction of a different term in a different statute, particularly when the statutes have different purposes, as these have. “Biographical information” which identifies a subject may be convenient shorthand for identifying some material which directed surveillance may disclose, but it does not cover, for example, a subject’s relationships with others which are part of private and family life.

130. For example, a tracking device, appropriately authorised, which shows a driver visiting his mistress’s address, his children’s school, his bank or any other premises unconnected with crime is likely to give rise to a breach of Article 8 even though these details may not be “biographical information” as defined in *Durant*: it should therefore be authorised as directed surveillance if there is to be RIPA protection.

Central Record of authorisations
131. Paragraphs 8.1 to 8.4 of RIPA and paragraphs 3.14 and 3.15 of RIP(S)A Covert Surveillance and Property Interference Codes of Practice and paragraphs 7.1 to 7.7 of RIPA and paragraphs 3.13 to 3.16 of RIP(S)A CHIS Codes of Practice, detail the requirements for a centrally retrievable record of all authorisations to be held by each public authority. Some aspects of covert policing are especially sensitive and require strict application of the ‘need to know’ principle (e.g. investigations into suspected police misconduct by a force Professional Standards Department, anti-corruption investigations and Special Branch operations). Authorisations (i.e. the document that provides the detail of the activity and the signature of the Authorising Officer) arising from these sensitive matters may be held in separate systems, away from the general run of authorisations, so long as they are centrally retrievable, are accessible to at least the Head of the Central Authorities Bureau (or equivalent unit), in order to ensure proper quality control, and are made available for examination by the relevant Surveillance Commissioner or OSC Inspector.
[36]

132. Full compliance is no mere bureaucratic requirement but will allow the person responsible for the Central Record, at a glance, to exercise effective oversight and quality control. It will enable that person to identify when reviews, renewals and cancellations are due, which Authorising Officer is directly involved in any of the operations which they authorise, and will draw attention to investigations likely to involve confidential information.

133. There should be a single centrally retrievable record, preferably in a tabular or electronic format, which contains the information required by the legislation. This record must include references to all the covert activities authorised by a prescribed officer of the authority. Any specialist units applying the 'need to know' principle may retain their own authorisations but must record the Unique Reference Number and key details of the authorisation on the single Central Record.

134. It is acceptable to have a Central Record for all CHIS activity (other than those authorised by the Security Service) and a separate Central Record for all other types of covert surveillance. It is also prudent to maintain a record of PA97 authorisations for property interference in the same place as the record for intrusive surveillance.

135. Local authorities may wish to have a single Central Record to record all covert activity given the smaller levels of usage. It would be sensible for this to include the details of any magistrates' approval under section 32(A) of RIPA.

136. Police Act 1996 collaboration agreements should make explicit provision for the proper keeping of a Central Record. In principle, the Central Record should be maintained by the force providing the Authorising Officer or the designated lead force. If an authorisation is enacted under the terms of a collaboration agreement, it is useful to refer to this on the Central Record of authorisations.

The use of template entries

137. Template forms inevitably lead to, or at least give the appearance of, minimal or no consideration of: (a) the nature and extent of the surveillance proposed and the justification for the use of the devices to be employed; (b) necessity; (c) proportionality; (d) collateral intrusion; and (e) what alternative methods have been considered. Template entries are therefore to be avoided or used with great care.

(See also Notes 67 to 69 and 99) [37]

Overseas Surveillance - Schengen Convention

138. Cross-border surveillance is now regulated under the Schengen Convention. Article 40.1 allows officers from one contracting party who are carrying out surveillance to continue that surveillance in the territory of another party where the latter has authorised the surveillance in response to a request for assistance. There are administrative provisions dealing with how and to whom requests for assistance should be made, and there is also provision for the surveillance to be entrusted to officers of the party in whose territory it is to be carried out. RIPA and RIP(S)A will apply in such a case in the UK.

139. Article 40.2 permits the officers carrying out surveillance in one territory to continue it across the border of another territory, where “for particularly urgent reasons” prior authorisation cannot be requested. This permission is subject to a number of conditions, including the requirement for officers to carry identification, make reports, etc. Those which seem significant are as follows:

139.1 Article 40.2 requires that the appropriate authority in the territory where the surveillance is being carried out should be notified immediately that the border has been crossed, and that a request for assistance should be submitted immediately, explaining the grounds for crossing the border without prior authorisation.

139.2 Article 40.2 further requires that the surveillance must cease as soon as the contracting party in whose territory it is being carried out so requests or, where no authorisation is obtained in response to the request mentioned above, five hours after the border was crossed.

139.3 Article 40.3.c provides that entry into private homes and places not accessible to the public is prohibited.

139.4 Article 40.3.d provides that the officers carrying out the surveillance may neither challenge nor arrest the person under surveillance.

Surveillance outside the UK (RIPA section 27(3))

140. Although under RIPA section 27(3) conduct may be authorised outside the United Kingdom, the application for such an authorisation calls for the exercise of judgment by the applicant because it could only be relevant in the United Kingdom (see Note 162). In case of doubt it is good practice to apply for an authorisation. [38]

Use by officers of covert surveillance devices to confirm at a later date what has been said or done by another person (section 48(2) of RIPA and section 31(2) of RIP(S)A)
141. In IPT/A1/2013 the IPT decided on 24 July 2013 that the covert making of a "voluntary declared interview" in the course of an investigation or operation is not surveillance within the meaning of Part II RIPA.

Length of applications
142. Applications for covert activity should be concise and should only contain material facts. This applies especially to intelligence cases.

143. The issue is one of balance, the object of OSC observations is not to restrict the information to be provided but to achieve a focus on what is really material and avoid burdening the process with information that is not relevant to the decision which is being made.

144. If it aids clarity and reduces reliance on powers of expression, sketches, annotated maps or photographs may be attached to documentation providing they are properly cross-referenced within the main document. Authorising Officers should sign attached documents and ensure that there is adequate information to collate documents if they separate.

Serious crime (section 93(4) of PA97 and section 81(3) of RIPA)
145. An authorisation for property interference cannot be obtained for an operation that does not concern 'serious crime'. If there is uncertainty about whether or not crime is 'serious', it is good practice to seek an authorisation.

Notification signatures
146. Although it is desirable, in exceptional circumstances it may not be necessary for a written notification to a Commissioner to be signed. The name of the Authorising Officer must always be clearly stated.

Collateral Intrusion
147. When notification of property interference is made to a Commissioner, details of any collateral intrusion (interference with persons who are likely to be affected by the interference) that may result as part of it or from use of any equipment put in place must be made known to the Commissioner at the same time. The matters covered by section 7.18 of the Covert Surveillance and Property Interference Code of Practice must be included in the application.
[39]

Renewals for property interference and intrusive surveillance must specify all actions taken

148. Commissioners do not see review forms so it is important that renewals for property interference and intrusive surveillance summarily specify all actions taken and material discovered since the previous authorisation was granted.

Continuing interference (sections 92 and 93(1)(a) of PA97)

149. The continuing presence of a surveillance device placed on any private property, including dwellings, hotel bedrooms and private or hired vehicles, is to be treated as a continuing interference. The wording of PA97 (and RIPA or RIP(S)A)) authorisations for surveillance equipment must cover its continued presence.

150. In the event that surveillance equipment is considered to be *lost*, and if all attempts to locate the equipment have been exhausted, the existing property interference authorisation and any associated authorisation may be cancelled. The Chief Surveillance Commissioner should be informed immediately in writing. Should the equipment's location subsequently be identified, a new property interference authorisation should be granted to enable the removal of the equipment as soon as its location is known and the Chief Surveillance Commissioner informed.

151. In the event that equipment is *irretrievable* a property interference authorisation should remain extant until its recovery is possible and any other surveillance authorisation should be cancelled. In extraordinary circumstances, when recovery is unlikely within a reasonable period, the Chief Surveillance Commissioner should be informed in writing detailing the circumstances and requesting permission to cancel the property interference authorisation. In this circumstance, interference continues but the equipment is not being authorised for the purpose of surveillance. If an opportunity to recover the item appears, a new property interference authorisation should be granted. As soon as the equipment is recovered the Chief Surveillance Commissioner should be informed in writing.

Property details (paragraphs 7.6 and 7.7 Covert Surveillance and Property Interference Code of Practice)

152. Interference is "properly authorised" when all property that may be interfered with is identified. It is important that any entry to surrounding property needed to achieve the objective is defined as clearly and as narrowly as possible. A Commissioner will not regard anything that is not specifically mentioned in the authorisation as being authorised.

153. When describing land to be entered, care should be taken to provide Commissioners with sufficient detail to permit the land to be clearly identified (e.g. O.S. grid references with plans showing them and the relevant land).
[40]

The effect of section 48(3)(c) of RIPA
154. Surveillance is defined to exclude the product from the interference with property. Searching a vehicle or baggage or placing a device in or on property is interference with it but it is not itself surveillance. There is a difference between activity which a trial judge may consider *"de Minimis"* and continuing interference which may provide a profile over time. The use of product from interference may be surveillance and should be separately authorised.

(See also Note 173)
Specify the interference
155. Property Interference authorisations must specify the interference. For example, a search would be authorised as "entry into X address and the recording or copying of any contents believed to be relevant to the investigation into the murder of Y".

156. Interference relates to the deed and is not confined to the purpose. Therefore, there is an expectation of authorisation when property is interfered with during feasibility studies or reconnaissance.

Property interference outside designated operational areas of responsibility when no written collaboration agreement exists
157. All that can be authorised outside a force area is the maintenance and retrieval of equipment. Entry on private land is not covered. Removal of a tracking device to replace its batteries or redeployment of identical equipment amounts to maintenance of the equipment, rather than replacement, and so can take place outside the Authorising Officer's force area, provided that the maintenance was authorised originally. If a property interference authorisation is intended to cover maintenance and retrieval outside the authorisation force area, the Authorising Officer must specify this: see PA97 (as amended) section 93(1)(a). This only extends to entry onto public land to carry out these actions. If entry onto private land outside the Authorising Officer's force area is required, the Authorising Officer of the force area within whose area the land lies must give the authorisation.

158. Any other interference with property or any entry on to private land cannot be authorised outside the force's own area. Any such authorisation has to be sought from the Authorising Officer of the area concerned. Authorisations from outside forces, in particular when property interference is sought, should be accompanied by the supporting directed surveillance authorisation, technical feasibility reports and a comprehensive map indicating where deployment is to take place.
[41]

The use of tracking devices
159. Attaching or placing a tracking device onto, or remotely obtaining information about the location of, property without the consent of the owner and when the property is not owned by the investigating authority is interference with property. The usual need to relate the location data obtained by the device to other information causes a potential and foreseeable invasion of privacy even if the location data is historical. In these circumstances it is necessary to obtain a property interference authorisation (to interfere with the property) and usually a directed surveillance authorisation (to make effective use of the product).

Tracking devices and surveillance equipment within public authority vehicles
160. Placing tracking devices or surveillance equipment in or on vehicles owned by the public authority entails no property interference by the authority. The use of a tracking or recording device is unlikely to be regarded as covert if the staff using the vehicle or device are appropriately notified that they are in place for the purpose of recording movements or for safety but may also be used for evidential purposes should the need arise. If equipment is issued to a member of the public authority and used for a purpose not notified to the vehicle occupants this use is covert and an appropriate authorisation should be sought. If a device is installed to covertly monitor, record, observe, or listen to other occupants an authorisation for directed surveillance is required.

Separate authorisations for each property interfered with
161. Separate authorisations are normally required for each property entered or interfered with in order to ensure that full consideration is given to whether each interference is warranted. The only exceptions are:

161.1 where all the properties concerned are owned by the main subject under investigation and it makes administrative sense to combine them. This may cover searches of rubbish at more than one address, if the main subject frequently moves home, or entry on property in order to carry out a feasibility study and subsequently or at the same time deploy technical equipment. However, it is not good practice to combine authorisations where part may require cancellation whilst part continues to be needed. Thus a private dwelling and a vehicle, even if belonging to the same person, would require separate authorisations.
161.2 where a subject has access to more than one vehicle, in which case the application can cover as many vehicles as is necessary, if such a wide authorisation is shown to be needed. Such authorisations will normally only cover one subject unless more than one subject uses the same vehicles. All vehicles must be identified whenever it is possible to do so. [42]

161.3 where an operation requires entry on or interference with more than one property in order to achieve the main objective, for example when officers need to cross various pieces of land to reach the property they wish to enter or interfere with, or where there is a need to enter private land to attach a tracking device.
161.4 where a subject is expected to book into one of two or more hotel rooms or two subjects are likely to book into different rooms in the same hotel.
161.5 where persons are suspected of joint involvement in a criminal enterprise.
(See also Note 119)

Overseas surveillance - subject nationality

162. An authorisation under RIPA is required whenever surveillance is carried out overseas by law enforcement agencies either directly or by others on their behalf. But where a subject is neither a UK national nor likely to be the subject of criminal proceedings in this country, and the conduct under investigation would neither affect a UK national nor give rise to material likely to be used in evidence before a UK court, such authorisation is not required.

Overseas deployment of VTDs

163. If a vehicle is expected to be travelling through several countries, it is sufficient for the authorisation to state that the deployment has the approval of the host countries without need for an authorisation for each country. If maintenance or retrieval of surveillance equipment whilst the vehicle is overseas is foreseen, then the authorisation should enable this action to be taken.

Extra-territorial offences

164. In relation to offences committed abroad, any actions under the provisions of Part III of PA97 may be undertaken in the United Kingdom only where the serious crime, in the prevention or detection of which such surveillance is likely to be of substantial value, consists of conspiracy to commit offences outside the United Kingdom [see sections 5, 6 and 7 of the Criminal Justice (Terrorism and Conspiracy) Act 1998].
[43]

165. Section 27(3) of RIPA provides that the conduct which may be authorised under Part II includes conduct outside the UK. A request for authorisation for surveillance in a Convention State would therefore be competent in terms of UK legislation. However, Article 40 of the Schengen Convention clearly restricts surveillance in the territory of any Convention State and Article 40.3.c, in particular, restricts intrusive surveillance. If any request for authorisation for surveillance in such a State which is party to the relevant provisions of the Convention is made, it should make clear how the surveillance is to be carried out consistently with the Convention, and what steps are being taken to request assistance from the State in question.

Urgent prior approval cases

166. A case is to be regarded as one of urgency within the meaning of the statutory provisions where either (a) the time taken to apply for the approval of a Commissioner, or (b) the further delay following at least one unsuccessful attempt to communicate with a Commissioner, or (c) inability to communicate securely with a Commissioner on account of mechanical failure, would in the judgment of the Authorising Officer, be likely to endanger life or jeopardise the operation in connection with which the surveillance is to be undertaken. A decision to give an authorisation under these circumstances must be notified to a Commissioner as soon as practicable after it is taken even if this is outside normal working hours (but not between 11pm and 7.30am).

Urgent oral authorisation (section 43(1)(a) of RIPA, section 19(1)(a) of RIP(S)A and section 95(1) of PA97)

167. For the purposes of sections 43(1)(a) of RIPA, 19(1)(a) of RIP(S)A and 95(1) of PA97, a case is to be regarded as urgent, so as to permit an authorisation to be given orally, if the time taken to apply in writing would, in the judgment of the person giving the authorisation, be likely to endanger life or to jeopardise the operation for which the authorisation is being given.

168. Paragraph 5.9 of the Covert Surveillance and Property Interference Code of Practice extends RIPA to include the requirement for the Authorising Officer as well as the applicant, when using the urgency provisions, to record the details set out in that paragraph. The Covert Human Intelligence Source Code of Practice (paragraphs 5.12 and 5.13) requires less information to be recorded and then only by the applicant. The Commissioners advise that, in addition to the details set out in the codes of practice, the key issues of necessity, proportionality, collateral intrusion and explicitly what has been authorised should be recorded.
[44]

169. Both codes require an urgent oral authorisation to be recorded when "reasonably practicable". The Commissioners advise that notes are made contemporaneously. If, at a later stage, the oral authorisation is recorded in another form (e.g. electronically) care should be taken to copy the contemporaneous notes precisely and not refer to the decision in the past tense. The same considerations apply to the notes and formal records completed by the applicant.

What constitutes 'property' and 'interference' (section 92 of PA97): keys, shoes, baggage searches and computer passwords

170. "Property" includes personal property such as keys and mobile phones.

171. If a computer is set up to work with a password, interference with the password requires an authorisation for property interference. An authorisation under Part III RIPA will be necessary if the owner is required to disclose the password.

172. Taking shoes away for prints is interference, unless authorised under another enactment, whereas taking impressions left after a person has trodden on a mat would not be, provided, of course, that access to the mat was lawful.

173. Deliberately holding up other people's baggage in order to avoid the suspicion of the subject as part of the operational plan to search his luggage constitutes interference. The activity may be considered *"de Minimis"* by a trial judge but it should be referred to in authorisations.

174. If software is installed in the computers in an internet café with the consent of the owner in order to determine when a known password is entered, an authorisation for property interference is not required, as the persons using the consoles do not have ownership of this property.

Interference (section 97(2)(a) of PA97)

175. Touching or pushing a door or a window, or putting a probe into a lock of a dwelling, office or hotel bedroom constitutes interference with that property and requires a Commissioner's prior approval before being undertaken.

Multiple vehicles used by a subject of surveillance

176. An authorisation may be expressed to permit interference with any vehicle which the subject may use and any vehicle into which the goods targeted may be transhipped. But such a formula should not be used except in relation to vehicles that cannot be further particularised.

Boats

177. Where it is possible that crew members of a boat may change, it is only necessary to name the owner in an authorisation relating to it.
[45]

Placing a device in a vessel (section 97(2)(a) of PA97)
178. Where devices are located on parts of a vessel which, arguably, are not used as a dwelling (such as the engine room) the safer course is nevertheless to seek prior approval.

Covert search of residential premises or a private vehicle and of items found therein (section 26(3-5) of RIPA and section 1(3-5) of RIP(S)A)
179. When a covert search of residential premises or a private vehicle is authorised under PA97 Part III a separate relevant RIPA Part II surveillance authorisation may be required to exploit information that is obtained as a result of that search. A covert search is unlikely to involve monitoring of "anything taking place" at the time of the search and is unlikely to be construed as intrusive surveillance; an authorisation for directed surveillance enabling the examination of items found during the covert search should suffice. Providing an authorisation to interfere with property and an authorisation for directed surveillance enabling the covert examination of items found exists, the location of the examination is irrelevant. A Senior Authorising Officer, when granting property interference, should make clear that he has ensured that a relevant RIPA Part II authorisation enabling the use of the product of the interference was extant at the time the authorisation was granted.

The use of surveillance devices on police property, in places of detention or custody and places of business of a professional legal adviser
180. Covert surveillance carried out in relation to anything taking place on so much of any premises specified in paragraph 4.18 of the Covert Surveillance and Property Interference Code of Practice as is, at any time during the surveillance, used for the purposes of legal consultation, is directed surveillance but shall be processed in the same way as intrusive surveillance (see Statutory Instrument 2010/461) and requires the prior approval of a Surveillance Commissioner. This can only be sought by a law enforcement agency. Surveillance carried out in these places when they are unlikely to be used for the purpose of legal consultation, should be authorised as directed surveillance.

181. Ordinarily a subject should have been interviewed before there is any recourse to listening devices, unless the Authorising Officer believes that further interview(s) will not progress the investigation.

182. When approval is sought for the deployment of surveillance equipment in a room on police premises that has been allocated exclusively to another partner agency or individual for their permanent use it may be expedient to seek a property interference authorisation and a directed surveillance authorisation. In the case of the room being used for legal consultations, the directed surveillance authorisation must be treated as intrusive surveillance and requires the approval of a Commissioner.
[46]

Police cells and prison cells (section 97(2)(a) of PA97)
183. No authorisation for property interference is needed for the placing of an audio or video device in a police or prison cell, provided that verifiable consent has been given by the Chief Constable of the appropriate force or by the officer in charge of the cell area.

Items seized under PACE
184. PACE enables overt seizure, examination and retention; it confers lawful possession but does not confer ownership or cover replacement or addition or continued use. However lawful the seizure, examination or retention may be, replacing or adding items or continuing to use the property is an interference with the property of another. PACE does not enable covert surveillance or interference. See also Notes 192-201.

Examination of mobile phones
185. Section 32(9)(b) of PACE, which only applies to arrested persons, allows a constable to retain anything not subject to legal privilege if he has reasonable grounds to believe that it is "evidence of an offence or has been obtained in consequence of the commission of an offence". This provision relates to offences already committed. It cannot extend to anything believed to reveal useful intelligence, the gathering of which will usually be at least part of the purpose of the examination. Section 54(5) of PACE requires that where anything is seized, the person from whom it is seized shall (except in two specified circumstances) be told the reason for the seizure. Ordinarily the purpose will be considerably wider than officers would want the suspect to be told. The examination of any mobile phone will generally be likely to lead to the acquisition of at least some private information. For these reasons, before examining a mobile phone covertly it is prudent to obtain authorisations for both property interference and directed surveillance. The Authorising Officer must be explicit when completing the authorisation regarding what is allowed (e.g. view or extract) and what is to happen in specified circumstances (e.g. when texts or voicemail arrive). Simple references to "examination" or "interrogation" are insufficient. Subject to Note 186 below, authorisations cannot, generally, authorise the opening of stored and accessible voicemail messages or texts whether or not already opened by the recipient. Access to data still in transmission is an interception (see *R v Coulson [2013] EWCA Crim 1026* paragraph 27 which interprets RIPA section 2(7) widely, although CACD were dealing only with voicemail, not texts).

not texts).

186. RIPA section 1(5)(c) makes lawful access to a stored communication for obtaining information in the exercise of some statutory power, e.g. – property interference under the Police Act 1997 or under PACE 1984. In this particular scenario, no directed surveillance authorisation is needed in addition to the property interference authorisation when downloading [stored] data from a device.
[47]

187. The Commissioners are aware that technology is capable of automatically downloading data even though there is no requirement for that data. If it is not possible to control what is downloaded, the use of such equipment should be avoided or the Authorising Officer should restrict the use of product obtained.

Refuse in dustbins (section 92 of PA97)

188. Refuse made available by the occupier of premises for collection by the local authority in dustbins or disposable bags or any other container, whether on private property or in the street, is to be regarded as having been abandoned by the occupier only in favour of the local authority, and it accordingly remains "property" within the meaning of the section.

Items or samples discarded in a public place

189. Where a subject discards an item belonging to him that the police may wish to retrieve in a public place (e.g. for DNA analysis), an authorisation for property interference is not required if the proper inference is that it has been abandoned. However, if a DNA sample is to be taken from property owned by another (for example a glass in a public house) it would be prudent to obtain the consent of the owner of the glass or seek authorisation if such an event could reasonably have been foreseen.

Surveillance devices installed in moveable property

190. Where a surveillance device capable of recording or obtaining private information installed within moveable property (e.g. a parcel or a briefcase) is to be taken into residential premises or a private vehicle, a PA97 authorisation for the "entry" of the device into those premises or the vehicle should be obtained. If the premises are either a dwelling or a hotel bedroom, prior approval of a Commissioner will be required. If the device is to be put into movable property without the property owner's consent, then an authorisation for the installation of the device should also be included.

191. An authorisation for intrusive surveillance need not be obtained just in case a device contained within movable property (e.g. a parcel or a briefcase) ends up in residential premises or a private vehicle. The possibility of a surveillance device, capable of recording or obtaining private information, being introduced into either of these places must be considered at the outset of the operation and a realistic view taken about the need for such authorisation.

[48]

Controlled deliveries

192. In the Commissioners' view, in all scenarios whereby an item is to be opened or otherwise interfered with during the course of its onward delivery, without the knowledge of the intended recipient, even if lawfully seized under another power, a property interference authorisation is required. This should include where the contents are extracted for further analysis, and where a substitute item or substance is inserted.

193. Holding or seizing a package during its transit under other statutory powers does not confer ownership (even if the true ownership is unknown or unclear). Suggesting that an illegal commodity can have no "owner" is not an argument accepted by the Commissioners.

194. A property interference authorisation is also required for the insertion of any trigger device, tracking device, and/or recording device.

195. Where such inserted items are likely to be delivered to, or end up within, residential premises or a private vehicle, the property interference authorisation should cater for this (with prior approval for any hotel, office, dwelling or where a recording device may capture confidential information).

196. Where a recording device, light meter or trigger device is likely to end up within residential premises or a private vehicle, then an intrusive surveillance authorisation will also be required.

197. A directed surveillance authorisation is likely to be needed for the later analysis or download of material/recordings/data obtained by means of the initial interference or activation of the device thereafter.

198. In the case of a "dummy package" (whereby a seized package and contents are replaced entirely by a substitute), no property interference authorisation is required in relation to that package, as it is entirely the property of the law enforcement agency in question. However, if any trigger device or such is inserted, then the necessary authorisations should be obtained as per above Notes.

199. If, for the purposes of a controlled delivery, a device is used purely to track an asset in order not to lose "sight" of it, and the data is not going to be used for evidence or to assist in the construction of intelligence, a directed surveillance authorisation may not be required. The relevant legislation is protective: it shall not be unlawful if an authorisation is obtained; it *may* be unlawful if it is not.

200. Every case should be considered on its individual merits. Law enforcement agencies should use their judgment (and seek necessary legal advice as desired) as to whether to seek an authorisation under the Police Act 1997 or RIPA/RIP(S)A. [49]

201. It will be sensible to record the rationale for not authorising any activity, as the Commissioners think that whilst it is unlikely that a trial judge would exclude the evidence in the absence of an authorisation, the law enforcement agency must be ready to show that it had acted in good faith in not having one.

Substantial financial gain (section 93(4)(a) of PA97)

202. “Substantial financial gain” is not defined in either of the Acts. Had Parliament intended this to be a fixed amount for every case it would have said so. In each case it is a matter of judgment by the Authorising Officer whether, taking into account all of the circumstances, the resulting gain is substantial.

203. What is to be considered is belief about resulting gain, not resulting profit. A drug supplier who buys drugs for £500 and sells them for £1,000 gains £1,000 from his supplying. The view may be reasonably taken that a burglar who steals jewellery valued at £1,000 gains £1,000, whether or not he then sells it for £100 or throws it away and whether or not what he throws away is recovered and returned to the loser.

204. In most cases the gain will be that of the offender(s), but gain to others criminally involved is material if it is believed to result from the conduct in question.

Victim communicators

205. When victim communicators or couriers are used in a kidnap or extortion situation, and surveillance equipment is deployed, a RIPA/RIP(S)A authorisation may not be required but, as so much depends on whether or not a crime is in fact being committed and on the scope of the surveillance being proposed, it would, in most cases, be prudent to obtain the appropriate RIPA/RIP(S)A authorisation.

Dwelling (section 97(2)(a) of PA97) and residential premises (section 48(1) of RIPA and section 31(1) of RIP(S)A)

206. PA97 concerns dwellings; RIPA and RIP(S)A concern residential premises. In both cases authorisation for property interference is required and, in the case of dwellings, prior approval of a Commissioner is necessary. The Acts are concerned with use at the time, not permanence.

206.1 Dwelling Prior approval is necessary where any of the property specified is used wholly or mainly as a dwelling (i.e. as a place of abode). Authorisation is therefore necessary for caravans, houseboats, yachts, railway arches, walkers’ hides, tents and anywhere else believed to be used as a place to live. An integrated house garage should be regarded as a dwelling. The parts of the premises subject to interference should be specifically identified in the authorisation. [50]

206.2 Residential premises Authorisation for intrusive surveillance is necessary for activity on residential premises involving the presence of an individual or a surveillance device. Hospital wards and police cells are likely to be residential premises but gardens and driveways are not. The parts of the premises subject to interference should be specifically identified and this will determine whether authorisation for intrusive or directed surveillance is appropriate. A lorry with sleeping accommodation should be regarded as residential premises requiring authorisation for intrusive surveillance. Absent any sleeping accommodation, authorisation for directed surveillance will usually suffice for a lorry.

Hotel bedrooms (section 97(2)(a) of PA97)

207. Property Interference authorisation should be given and the prior approval of a Commissioner obtained for any interference with or entry into a hotel bedroom, whether devices are installed before or after allocation, signing the register or entering the room. Even if a device is fitted with the consent of the hotel owner or manager prior to the subject(s) taking occupancy, a property interference authorisation and the prior approval of a Commissioner are still required for the continued presence of the device and any servicing or retrieval of it whilst the room is allocated to the subject.

Interference with leased premises

208. Property leased to a public authority by tenancy agreement does not make the public authority the owner. Without the consent of the owner or a permitting lease, the fabric of such property may only be interfered with (for example by way of installing a listening device or drilling a hole to insert a probe to monitor neighbouring property) after authorisation for property interference and an associated intrusive or directed surveillance authorisation.

Repeat burglary victims and vulnerable pensioners

209. While the consent of the owner to the installation of a surveillance device on his premises avoids the need for a property interference authorisation, the Authorising Officer should consider whether it is likely that the privacy of another person lawfully on the premises may be invaded. Any visitor who is not made aware of it is subject to covert surveillance. This is a technical breach of the visitor's Article 8 rights, although in such circumstances any complaint may be regarded as unlikely.

210. The surveillance is intrusive because it is carried out in relation to things taking place on residential premises: section 26(3)(a). But if the crime apprehended is not "serious", intrusive surveillance cannot be authorised: *cf* section 32(3)(b). On the other hand, the surveillance is not directed, because it is intrusive: section 26(2). [51]

211. The fact that particular conduct may not be authorised under RIPA or RIP(S)A does not necessarily mean that the actions proposed cannot lawfully be undertaken, even though without the protection that an authorisation under the Acts would afford.

212. The Investigatory Powers Tribunal (IPT) has provided clear advice in its judgment in *Addison, Addison & Taylor v Cleveland Police* (IPT/11/129/CHIS; IPT/11/133/CHIS; and IPT/12/72/CHIS) that where no authorisation is capable of being granted in such circumstances, "it will behove a police force to follow a course similar to that adopted here; i.e. a procedure as close as possible to that which would be adopted if an authorisation could be obtained from a Chief Constable [for intrusive surveillance] or other relevant Authorising Officer." The IPT also warned that whilst the conduct in question might be unprotected by an authorisation (as none can be given), that conduct might still be scrutinised by the IPT, and as such, it might not be appropriate to describe any relevant Article 8 breach as "technical".

Binoculars and cameras (section 26(5) of RIPA and section 1(5) of RIP(S)A)
213. If binoculars or cameras are used in relation to anything taking place on any residential premises or in any private vehicle the surveillance can be intrusive even if the use is only fleeting. It will be intrusive "if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle". The quality of the image obtained rather than the duration of the observation is what is determinative.

Stolen vehicles (section 48(1) of RIPA and section 31(1) of RIP(S)A)
214. A stolen vehicle is not a "private vehicle" for purposes of the Acts because a private vehicle is defined by these provisions by reference to use by the owner or person who has the right to use it.

215. When it is intended covertly to track a stolen vehicle, the terms of the legislation can properly be met if regard is had to the following considerations:

215.1 Each authorisation must expressly address proportionality, not only in relation to the interest of the public but also in relation to the owner, so the routine fitting of tracking devices is not permissible.
215.2 Proportionality includes consideration of the particular vehicle and will be affected by such matters as whether the owner has a particular need for the vehicle or its contents, whether the vehicle is likely to be damaged further and whether he has already been paid out by his insurers. (Information as to particular need could be obtained at the time of the original theft: The Commissioners recognise the problem of going back to the owner when fitting the tracking device is being considered.) Unlimited authorisations are unlikely ever to be proportionate. [52]

215.3 Early reviews are likely to be essential.
215.4 The urgency criteria will often be usable.
216. The Commissioners are liable to quash authorisations which are wide in scope and which do not relate to an identified stolen vehicle.

Automated Number Plate Recognition and CCTV lists of interest
217. The 'private life' of a car driver is not interfered with when the registration number of his vehicle is recorded by ANPR while he is travelling on a public road, because the registration plate is a publicly displayed object. It is not adequate to say that recording and storing data capable of identifying the occupants of the car does not require authorisation because they are in a public place: they are, but they are ignorant of the capacity of the camera and the extent to which the data may be retained and used. Some ANPR cameras are now capable of producing clear images of the occupants of a car, as well as the vehicle make and registration number and technology is available which is designed to defeat windshield glare. It is therefore possible to interfere with a person's private life. If the occupant is in a private vehicle such use of ANPR may in consequence constitute intrusive surveillance if data that is recorded for potential later use is capable of identifying him.

218. Monitoring and recording the movements of a specific vehicle or person (persistently or intermittently) over a protracted period or distance, when no action is taken to stop the vehicle or individual when first sighted, is capable of being directed surveillance and an authorisation should be obtained. If the details of persons or vehicles are placed on a list requiring that an investigating officer be notified or a record is made of the location or movements of the person or vehicle, or that vehicle or person is subjected to focused monitoring to build up a picture of the movements of the vehicle or person, an authorisation is expected.

219. It is not the general collection of images of number plates, or coincidental images of occupants, which concerns the Commissioners when interpreting RIPA and RIP(S)A. The reason for placing a vehicle or person on a list of interest, and the action to be taken when they are sighted, are crucial. For example, recording the details of a vehicle related to a traffic offence, where the intention is to stop the vehicle and talk to the driver when sighted, or providing a warning to police that a vehicle is related to offences involving violence are not directed surveillance; both are immediate reactions to events because it could not be foreseen that the vehicle would appear at the given time. However, placing the details of a vehicle or a person on a list because they relate to a criminal investigation or because they have the propensity to commit crime and, when sighted, observing them or placing the time and location on a log for later analysis, is directed surveillance. It follows that it is necessary to have separate lists depending on the action to be taken.
[53]

220. The person deciding to place a person or vehicle on a list of interest, where the activity is capable of being construed as covert surveillance, must be competent to make the decision (i.e. must hold the minimum grade, rank or office specified by legislation). If authorised, clear direction is required regarding review, renewal and cancellation (which must include the destruction of data if appropriate and instructions for removal from relevant lists).

Premises set up to monitor traders covertly

221. Premises set up solely for surveillance purposes and not occupied or in current use for residential purposes are not residential premises within section 26(3)(a) of RIPA and surveillance carried out there is therefore not intrusive but may require authorisation for directed surveillance. The position would be otherwise if a variety of devices were deliberately set up in premises which continued to be occupied for residential purposes (sometimes referred to as a "house of horrors"). In some cases, a CHIS authorisation may afford protection if the person purporting to be the occupant of the premises establishes or maintains a relationship with a trader and merits consideration depending on the facts.

Authorisation for undercover officers (section 29(4)(b) of RIPA and section 7(5)(b) of RIP(S)A, and Statutory Instrument 2013/2788)

222. With the advent of Statutory Instrument 2013/2788, which came into force on 1st January 2014, the emphasis has been placed firmly on the authorisation of individual undercover operatives instead of the wider operational activity upon which they are deployed.

223. It is the responsibility of law enforcement agencies to ensure that all authorisations and renewals of undercover officers, as defined within Statutory Instrument 2013/2788, and whose renewal beyond twelve months – or three months where there may be access to legally privileged material (article 8(1)(b) of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010) - now require the prior approval of a Surveillance Commissioner, are brought to the attention of the OSC. Notes 35-52 advise how this is to be done.

224. If a prior approval renewal, or the need for its notification at the nine-month stage, is overlooked, there may be limited time left in which to complete the necessary actions, or the operative's valid authorisation period may have already ended. In the latter case, a formal cancellation must be completed and a fresh authorisation (with the prior approval of a Surveillance Commissioner) sought. Where, through oversight, a prior approval renewal is sought from the OSC at very short notice, it shall be at the discretion of the Surveillance Commissioner whether this shall be progressed before the natural expiry date of the valid authorisation. (See also Notes 52-55)
[54]

225. More than one undercover officer can be included on a single authorisation document, provided they are individually identified by their unique national index number from the outset. In this case:

225.1 The application and authorisation should clearly address the necessity and proportionality of using multiple operatives, and the collateral intrusion considerations.
225.2 A risk assessment must be completed, pertinent to each individual, which takes into account all the circumstances of the environment in which each is to be deployed and the relevant experience of each operative. This should reflect all other covert activities in which that officer has been, or is contemporaneously, engaged and the level of training the officer has received. This is particularly relevant if the undercover officer comes from a different force, public authority or third party, including from an overseas force. Police collaboration agreements should make arrangement for these details to be made available.
225.3 The Surveillance Commissioners will expect, as a matter of good practice, to see that a risk assessment has been signed or initialled by those holding the section 29(5)(a) and 29(5)(b) roles, and by the Authorising Officer, who should add any relevant comments to the risk assessment form. The Surveillance Commissioners also advise that it is good practice for an Authorising Officer to sign and date each page of the application form to evidence their consideration.
225.4 The Authorising Officer must set out in clear, unequivocal terms, the use and conduct authorised for each individual operative. Particular care is needed where a single authorisation document includes conduct for Foundation and Advanced operatives.
225.5 Where participating conduct is intended for undercover officers, the Surveillance Commissioners are content that if the conduct has been authorised under Part II of RIPA/RIP(S)A it will be lawful for all purposes, as per section 27 of RIPA and section 5 of RIP(S)A. However, the Authorising Officer must stipulate in explicit terms what exactly the undercover officer is authorised to do. Record should also be made (and thus provided) as to what advice has been given by the CPS (PFS in Scotland).
225.6 The records should show clearly which officers hold the roles for the individual undercover officer(s) under section 29(5) of RIPA and section 7(6) of RIP(S)A. [55]

226. An initial authorisation wording can include that, if operationally necessary, additional undercover officers can be authorised. However, each new undercover officer must be authorised formally by way of a review document, or on a separate unique authorisation form, and the considerations of necessity, proportionality, collateral intrusion, and risk must be addressed per operative, and their parameters of engagement made clear. The authorising officer must also record the effective authorisation period applicable to each new undercover operative authorised in this way. (See also Notes 41 and 228)

227. Authorising Officers are responsible for ensuring that the correct authorisation dates for each individual undercover officer are recorded, mindful of the calculation requirements within Statutory Instrument 2013/2788.

228. Reviews of undercover officers' deployments cannot be delegated. Parliament has decreed that authorisations must be by the senior ranks identified within Statutory Instrument 2013/2788, and once authorised, those undercover officers' use and conduct and the duty of care owed to them remain the responsibility of that senior Authorising Officer. In "long term" authorisations, granted prior approval by a Surveillance Commissioner, the ongoing responsibility remains with the Chief Constable or equivalent and similarly, cannot be delegated.

229. If, during their current deployment, an undercover officer is provided with a new personal URN/National Index number, this must be made clear on the documentation and highlighted for the attention of a Surveillance Commissioner where a prior approval renewal is sought. The change in number must also, as soon as the change occurs, be provided to the London OSC office.

The need for an undercover officer authorisation

230. Every case must be considered on its merits, but in relation to the authorisation of the use and conduct of an undercover officer, the Surveillance Commissioners consider this is unlikely to be necessary in cases where there is so fleeting or minimal an engagement with a subject (whether or not identified) that the criteria for a CHIS authorisation are not met. Such examples may include the use of officers as decoys for street robberies; simple exchanges on Internet sites such as eBay to determine the availability of an item and to arrange its purchase (such as in the case of an identified stolen bicycle or counterfeit goods) – see also Note 239; or for simple controlled deliveries to an address, where the intention is to take executive action immediately and the engagement of any subject(s) within the context of the covert delivery is minimal. In every case, the matter should be determined by an Authorising Officer and a written record retained of the rationale for not obtaining a CHIS authorisation.
[56]

Use of directed surveillance for a prospective CHIS
231. An assessment of suitability is not usually an investigation of crime under PA97 or any of the other reasons cited in RIPA section 28(3) or 29(3) and section 6(3) of RIP(S)A. Although the use by a police force of covert surveillance to assess the suitability of a person to act as a CHIS cannot usually be authorised under RIPA or RIP(S)A, it should be capable of being justified under Article 8.2 of ECHR.

Pre-authorisation meetings with prospective CHIS
232. An intelligence debrief may not require an authorisation but any tasking to establish or maintain a relationship for a covert purpose or to test reliability may and should be kept under review by an Authorising Officer with appropriate log entries. In principle, it may be better to authorise early and then cancel, if it is later decided not to progress with the CHIS use and conduct, than it is to jeopardise the admissibility of evidence because an authorisation was not obtained. This should not be confused with the assessment of CHIS suitability where no tasking is involved (see also Note 231).

233. “Debriefing” in this sense means obtaining information which it is believed is already known by the person before initial contact. If it is likely that a person, after discussion with a member of a public authority, obtains information as a result of a relationship, which he knows or perceives to be of interest to the public authority, authorisation should be considered.

234. When an individual is rewarded for, or an intelligence report is submitted relating to, information which is used or disclosed in a manner calculated to ensure that the person(s) being reported on are unaware of the use or disclosure in question, the need for authorisation should be seriously considered.

Adult CHIS (including the majority of undercover officers and those authorised to participate in crime) require a full 12 months’ authorisation
235. All written authorisations for CHIS, unless they fall for authorisation under the long term authorisation arrangements of Statutory Instrument 2013/2788 or in accordance with the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010, should be of 12 months’ duration: *cf.* section 43(3) of RIPA and section 19(1(b)) of RIP(S)A. Reviews, on the other hand, may be conducted at whatever frequency the Authorising Officer deems appropriate (juvenile CHIS require one month authorisation).
[57]

Participating CHIS - level of authorisation
236. Notwithstanding the changes brought about in relation to the authorisation of undercover officers, the legislation prescribes the minimum rank or grade for an Authorising Officer granting the use of a CHIS. Some public authorities, in a desire to supervise this type of CHIS more closely, have stipulated a higher rank or grade officer. The legislation enables this but it does not enable an adjustment to the length of an authorisation (Statutory Instrument 2013/2788 excepted) and the Authorising Officer may not delegate all or part of his statutory responsibilities. In other words, there can only be one Authorising Officer per CHIS at any time and that person must be responsible for all aspects of use and/or conduct until that specified conduct (i.e. participation) is cancelled.

237. The Commissioners will not criticise an arrangement that retains the rank or grade of an Authorising Officer at the minimum prescribed level but which requires the Authorising Officer to inform a more senior officer of the necessity and proportionality of the use of the CHIS in this way. This will enable the senior officer to consider the corporate risk to the organisation (not the risk to the CHIS or the tactics involved) which will enable the Authorising Officer to make an informed risk assessment. It is imperative that the senior officer does not interfere with the Authorising Officer's statutory responsibilities by providing direction regarding authorisation.

CHIS – Sub-sources and conduits
238. Where the identity of a sub-source is unknown and information said to have been obtained from him/her is passed on to a public authority by a conduit, without the knowledge of the sub-source, the conduit is maintaining a covert relationship with the sub-source and should be treated as a CHIS.

Covert Internet Investigations - e-trading
239. CHIS authorisation is only required for the use of an internet trading organisation such as eBay when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage.

CHIS should not be dual authorised
240. The Covert Human Intelligence Source Code of Practice paragraph 2.9 refers to the potential that a single CHIS “may be subject of different use and conduct authorisations obtained by one or more public authorities” and that “such authorisations should not conflict”.
[58]

241. A public authority is not entitled to regard a CHIS as its own agent unless it has authorised him or her. For authorisation to be proper it must be given by an organisation with a single system of management. Put another way, there cannot properly be dual authorisation of an individual using more than one Authorising Officer or more than one authorisation for use: the risk of overlap and confusion is obvious and to be avoided. It is possible for an individual to be subject to different conduct authorisations proposed by different public authorities, but a wise Authorising Officer will endeavour to keep the number of simultaneous authorisations to a minimum by way of review (cancelling and combining conduct authorisations when appropriate).

242. The principle of minimising the number of Authorising Officers and authorisations for a single operation or investigation also applies to authorisations to interfere with property, directed surveillance authorisations and section 49 notices.

243. Covert Internet Investigators (now often referred to as undercover officers on line (UCOL)) may establish or maintain a relationship with more than one individual in relation to different investigations. If it is not possible to construct a single authorisation to cover all of the relationships (because the persons with whom relationships are established are not known in advance) it will be necessary to construct for each person with whom a relationship has been established a separate authorisation each of 12 months' duration. It is important that the same Authorising Officer considers each authorisation to ensure that operational conflict and risks do not develop, and to monitor the security and welfare of the CHIS. When appropriate, reviews should be combined to establish whether separate authorisations can be combined into a single authorisation to reduce bureaucracy and error.

Test purchase of sales to juveniles

244. When a young person, pursuant to an arrangement with an officer of a public authority, carries out a test purchase at a shop, he is unlikely to be construed as a CHIS on a single transaction but this would change if the juvenile revisits the same establishment in a way that encourages familiarity. If covert recording equipment is worn by the test purchaser, or an adult is observing the test purchase, it will be desirable to obtain an authorisation for directed surveillance because the ECHR has construed the manner in which a business is run as private information (see also Note 261 and Covert Surveillance and Property Interference Code of Practice paragraphs 2.5 and 2.6) and such authorisation must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person. [59]

245. When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent “fishing trips”. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been considered or attempted and failed.

246. There is a difference between test purchases to establish whether juveniles are sold goods illegally and a test purchase conducted by a law enforcement officer for the sale of drugs or stolen items. The latter is more likely to require authorisation for the use and conduct of a CHIS. The authorisation always relates to the CHIS relationship and not the operation. All CHIS should be properly risk assessed.

Handlers and Controllers must be from the same investigating authority as the Authorising Officer if no joint working agreement exists.

247. Paragraphs 6.10 to 6.13 of the RIPA CHIS Code of Practice relate to authorisations for the use or conduct of a CHIS whose activities benefit more than a single public authority. In circumstances where a single public authority is the beneficiary of the product obtained from a CHIS, the persons prescribed at section 29(5) of RIPA and section 7(6) of RIP(S)A (usually referred to as the Controller and the Handler) must be from the same investigating authority as the Authorising Officer, unless, in the case of specified law enforcement agencies, an agreement exists under the Police Act 1996 which enables alternative arrangements.

248. The Authorising Officer should carefully consider whether the simple passing of information resulting from a CHIS report is benefiting after the event or whether the benefit is contemplated at the time of authorisation. The Commissioners caution against the term 'beneficiary' being used as a convenience to share resources.

249. If a test purchase officer or undercover officer is accompanied by a cover/welfare officer the latter cannot fulfil the obligations under section 29(5)(a) if there is no written collaboration agreement enabling it.

Joint working – CHIS authorisations

250. The principles of authorisations subject to a collaboration agreement set out in paragraph 3.16 of the RIPA Covert Surveillance and Property Interference Code of Practice should be considered applicable to an authorisation for the use and conduct of a CHIS.
[60]

Local Authority CHIS
251. A local authority may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed (see CHIS Code of Practice 6.12). In the absence of such an agreement the local authority must be capable of fulfilling its statutory responsibilities.

252. Elected members and Senior Responsible Officers (see paragraphs 3.27 and 9.2 of the CHIS Code of Practice) are required to ensure that policies are fit for purpose and that Authorising Officers are competent. An elected member has no need to know the identity of a CHIS nor have access to the product of the use of a CHIS nor know the detail of conduct authorisations. Chief Executives may provide elected members with a copy of OSC inspection reports, redacted if necessary.

253. Some local authorities may not wish to use CHIS and may in practice avoid authorising CHIS. However, all such local authorities should recognise that the occasion may arise when a CHIS appears unexpectedly and has to be authorised and managed. Consequently, all local authorities must be equipped with a policy and the awareness training to recognise status drift.

The use of terms other than CHIS
254. The legislation does not envisage a different management regime for different types of CHIS. The term “Tasked Witness” is sometimes used to identify a particular type of CHIS who is willing to testify in court and police officers are variously undercover, test purchase, decoy or covert internet investigators. All types are entitled to all the safeguards afforded a CHIS and the public authority must provide them, including proper considerations for, and completion of, authorisations and risk assessments although some of the factors for consideration, for example when making a risk assessment, may differ as between a CHIS who is an employee of a public authority and one who is a member of the public.

CHIS - remote contact
255. Other than in exceptional and explained circumstances, it is important that regular face-to-face meetings form the primary method for meeting a CHIS rather than remote contact (for example by telephone, text messages or email). The Authorising Officer should question, on review and renewal, why reasonably frequent face-to-face meetings are not being conducted.
[61]

Monitoring of CHIS meetings
256. Overt recording of meetings with a CHIS may be made but the product should be properly recorded, cross-referenced and retained. The Authorising Officer should assess and manage the risk of disclosure of audio recordings which may compromise the identity of the CHIS.

Undercover officers - legend construction
257. During the construction of a legend an officer may establish or maintain a relationship with another person who is not the subject of an operation. The nature of that relationship may be for a covert purpose. It will be covert if it is not clear to the other person that the officer is not who he claims to be. The purpose may be to facilitate access to the subject of an operation or to facilitate *bona fide* checks later. If the relationship is for a covert purpose, and the activity relates to a current operation, an authorisation should be obtained. Where the legend is being prepared for possible later use an authorisation may not be necessary. Appropriate arrangements should be in place to manage “status drift”.

Repeat voluntary supply of information
258. Some individuals provide information but do not wish to be registered as a CHIS; others repeatedly provide information that has not been sought or where the public authority does not wish to authorise the individual as a CHIS (e.g. because there is evidence of unreliability). If the information being provided is recorded as potentially useful or actionable, there is a potential duty of care to the individual and the onus is on the public authority to manage human sources properly. The legislation is silent regarding consent but sensible procedures should exist to monitor for status drift and to provide the trial judge with a verifiable procedure. Authorising Officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose as described in paragraphs 2.10 to 2.25 of the CHIS Code of Practice.

Separate CHIS use and conduct authorisations
259. It is the practice of some public authorities to separate the use and conduct authorisations; there is nothing in the legislation to prevent this but it can lead to error. The principle is that there should be a minimum number of authorisations for a CHIS and each authorisation should stand on its own. Conduct authorisations should not conflict and care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant reviews, renewals and cancellations are correctly performed.
[62]

CHIS interference with property
260. Although it is not encouraged, it is permissible for CHIS to interfere with property (for example, by photocopying documents should an opportunity arise), provided that the terms of the authorisation contemplated this type of conduct. If property interference is foreseen, it would be prudent also to obtain an authorisation for this.

Extent of directed surveillance (section 26 of RIPA and section 1(2) of RIP(S)A)
261. Directed surveillance is covert surveillance that is carried out for the purposes of a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person, whether or not he is a subject of the action. It includes the activity of monitoring, observing, listening and recording by or with the assistance of surveillance equipment. It need not be subject specific. A search for an identified person in a public place will not amount to directed surveillance, unless it includes covert activity that may elicit private information about that person or any other person. Any processing of data (e.g. taking a photograph to put on record) is an invasion of privacy.

Subject or operation specific (section 26(2)(a) of RIPA and section 1(2)(a) of RIP(S)A)
262. Whether a fresh authorisation is required if new subjects emerge depends on the terms of the original authorisation. But in principle these provisions put the emphasis on the operation as being the purpose of the surveillance.

Immediate response (section 26(2) of RIPA and section 1(2)(c) of RIP(S)A)
263. These provisions explain the expression “an immediate response to events or circumstances” by saying “the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.” In short, it relates to events or circumstances that occur extemporarily. A response is not to be regarded as “immediate” where the need for an authorisation is neglected until it is too late to apply for it. See also RIPA Covert Surveillance and Property Interference Code of Practice paragraph 2.23.

Crime in progress: private information (section 26(10) of RIPA and section 1(9) of RIP(S)A)
264. As a general principle, if it is clear that a crime is in progress, the offender can have no expectation of privacy and no authorisation for directed surveillance will be required.

265. It is important to differentiate between a crime in progress and a criminal situation which is believed to exist but where evidence may be lacking. In the latter case it would be prudent to obtain an authorisation if time permits.
[63]

Describe the operation
266. Authorisations against a named subject should indicate when, where, and in what circumstances the surveillance is to be carried out.

267. Authorisations should specify only the specific covert activities or techniques likely to be required. (See also Note 99)

Pre-emptive directed surveillance authorisations
268. When high grade intelligence is received which enables the production of a plan involving covert surveillance, but where the exact details of the location are not known, it is permissible to prepare an authorisation in order properly to brief those conducting the surveillance. But it must be subject to an immediate review once the missing details are known. It is unwise to act on an incomplete authorisation and this guidance should not be construed as enabling authorisations to be regularly prepared in anticipation of events. The difference between this guidance and use of the urgency provisions is that the urgency provisions may only be used when events could not be anticipated and when there is a threat to life or the operation would be otherwise jeopardised.

Electronic surveillance across the Scottish/English border
269. There is no difference between the method of surveillance (electronic or non-electronic) and the same rules apply to each.

"Drive by" surveillance
270. "Drive by" surveillance may or may not need an authorisation and it is not acceptable to prescribe a minimum number of passes before an authorisation is required.
[64]

Use of noise monitoring equipment
271. Measuring levels of noise audible in the complainant's premises is not surveillance because the noise has been inflicted by the perpetrator who has probably forfeited any claim to privacy. Using sensitive equipment to discern speech or other noisy activity not discernible by the unaided ear is covert, likely to obtain private information and may be intrusive surveillance. The Authorising Officer should consider whether the surveillance equipment is capable of measuring volume only or whether it can identify the perpetrators; mindful that the more sensitive the equipment the greater the potential for intrusive surveillance. Where possible, the intention to monitor noise should be notified to the owner and occupier of the premises being monitored. Where notice is not possible or has not been effective, covert monitoring may be considered necessary and proportionate. If monitoring equipment is used as a means also to assess whether a claim is vexatious, any consent provided by the complainant to use monitoring equipment on his premises is vitiated if the full capability of the equipment is not explained.

(See Covert Surveillance and Property Interference Code of Practice 2.30)
CCTV systems - the need for a unified protocol for use
272. It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach. The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

Urgent oral authorisations - essential information to be provided to local authority CCTV managers
273. When an urgent oral authorisation has been issued, the local authority (or any other entity acting on the authorisation) should be provided with the details (including contact information) of the Authorising Officer, the start and expiry date and time and a written summary of what has been authorised (copy of contemporaneous notes taken by the applicant).

Surveillance of persons wearing electronic tags
274. If surveillance against a person wearing an electronic tag is done in a manner not made clear to him, that surveillance is covert and an authorisation should be obtained.
[65]

Recording of telephone calls - one party consent
275. Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, a telephone conversation (or other voice data communication such as Voice Over Internet Protocol) may be recorded and authorised as directed surveillance providing that the consent of one of the parties is obtained (see paragraph 2.9 of the RIPA Covert Surveillance and Property Interference Code of Practice). Providing that the original terms of a CHIS authorisation enables it, an additional authorisation for directed surveillance is not required if a CHIS sets out to overhear or record a telephone conversation or other voice data communication (see paragraph 2.30 of the RIPA Covert Surveillance and Property Interference Code of Practice). If there is doubt, it would be prudent to obtain a directed surveillance authorisation. There is no equivalent provision in RIP(S)A.

Closed visits in prison (section 48(7)(b) of RIPA)
276. In prisons closed visits take place in a common area in which booths are set up in such a way as to prevent contact between the inmate and visitor, or in which cubicles are provided in order to afford a limited degree of privacy primarily in relation to other inmates. But whatever form surveillance may take, such a visiting booth or cubicle is not a space being used for residential purposes or otherwise as living accommodation so as to amount to intrusive surveillance. If the surveillance is likely to obtain information subject to legal privilege it is directed surveillance but is authorised using intrusive surveillance processes.

277. Provided that notices are displayed within visiting areas advertising the fact that CCTV is in operation, a directed surveillance authorisation is not needed for visual monitoring of prisoners during open prison visits, as they will be aware that they are under surveillance. But when CCTV is concentrated on a particular visit or visits as part of a pre-planned operation, and private information is likely to be obtained, an authorisation should be applied for.

Crime hotspots (section 26(2) of RIPA and section 1(4) of RIP(S)A)
278. The statutory provisions apply to the obtaining of information about a person whether or not one specifically identified for the purposes of the investigation. It is not restricted to an intention to gain private information because the subsections refer to covert surveillance carried out “in such a manner as is likely to result in the obtaining of private information”.

279. Surveillance of persons while they are actually engaged in crime in a public place is not obtaining information about them which is properly to be regarded as “private”. But surveillance of persons who are not, or who turn out not to be, engaged in crime is much more likely to result in the obtaining of private information about them.
[66]

280. An authorisation for Directed Surveillance is required whenever it is believed that there is a real possibility that the manner in which it is proposed to carry out particular surveillance will result in the obtaining of private information about any person, whether or not that person is or becomes a subject of the operation.

(See also Notes 125-126)

Police use of grounds of national security (cf RIPA section 28(3)(a) and 29(3)(a))

281. RIPA enables a Chief Constable (using his Special Branch) to conduct activity on the grounds of national security. The Commissioners acknowledge the Security Service's primacy and would expect a law enforcement agency to offer that Service the opportunity to take the lead (i.e. to authorise). If this offer is rejected, the Chief Constable should not be constrained from investigating using his own resources providing that the grounds of proportionality and necessity are met. If he decides to authorise a CHIS on these grounds, without "concurrence", the CHIS should be managed in accordance with the legislation, codes of practice *and* OSC guidelines.

Surveillance equipment should be under central management

282. All surveillance equipment owned by the public authority should be under central management, since, whatever the object, covert use could be made of most devices. It is considered best practice to cross-reference equipment deployment records with the Unique Reference Number of the relevant authorisation. Where surveillance equipment is shared (e.g. partnership arrangements) there should be auditable processes to prevent unauthorised use of surveillance equipment.

The availability of resources

283. Whilst there may be a public expectation that public authorities will monitor offenders, an Authorising Officer should not grant an activity when he knows there to be insufficient covert surveillance resources to conduct it.

Technical feasibility studies

284. Feasibility studies should be conducted before the application is submitted to the Authorising Officer. Without it the Authorising Officer is unable to know the objectives can be achieved or to accurately assess proportionality or collateral intrusion. It is unacceptable to deny knowledge of technical capability from the Authorising Officer.
[67]

Copying property
285. To copy the owner's key would require a PA97 authorisation; to obtain duplicate keys from a manufacturer would not require an authorisation for interference with property but the use of them would require a PA97 authorisation.

Civilian Authorising Officers in law enforcement agencies
286. RIPA and RIP(S)A designate the minimum rank, grade or office of an Authorising Officer; for police force non-urgent authorisations the minimum rank is Superintendent. The omission of the words "or equivalent", which are used for other public authorities, suggest the omission is deliberate. Without amendment to legislation, law enforcement agencies are confined to serving officers. Should legislation be amended to enable a non-serving police officer, it is vital that an Authorising Officer is able to demonstrate competence equivalent to the minimum rank, grade or office specified.

Covert surveillance of cohabiting couples
287. The purpose of surveillance is to investigate a crime and not a criminal. It is usually not possible to be certain of a partner's awareness of a criminal situation and proving cohabitation is sometimes necessary and proportionate. The Commissioners believe that it is appropriate, subject to accurately constructed documents, to authorise surveillance against cohabiting parties. Authorising Officers should confine surveillance of the partner to that which is necessary to prove cohabitation. Surveillance of juveniles or other family members should be avoided.

The Senior Responsible Officer should avoid granting authorisations
288. The role of the Senior Responsible Officer is to oversee the competence of Authorising Officers and the processes in use in his public authority. Whilst legislation does not preclude his use as an Authorising Officer, it is unlikely that he would be regarded as objective if he oversees his own authorisations. For this reason, the Commissioners believe that the Senior Responsible Officer in a law enforcement agency should be of a minimum rank, grade or office equivalent to a Chief Officer (i.e. ACPO/ACPO(S) rank).
[68]

Covert surveillance of Social Networking Sites (SNS)

289. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

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

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done). [69]

Technical reconnaissance and feasibility studies
290. If it is likely that during the conduct of a reconnaissance or a feasibility study, property will be interfered with, or private information will be obtained, it should be authorised appropriately.

Updating photographs for intelligence purposes
291. Covertly taking a photograph for the purpose of updating records is capable of being directed surveillance and should be authorised.

Prior approval of a magistrate under section 32A of RIPA (England and Wales only)
292. The Commissioners consider that the best officer to apply to the magistrate for approval of an authorisation of directed surveillance or CHIS is the Authorising Officer, though they recognise that this is not always practicable. Only he can answer questions about his reasoning on necessity, proportionality, collateral intrusion and risk.

293. If the Authorising Officer is not present before the magistrate, any comments made by the magistrate should be promptly reported to him. Such comments might affect the future conduct of the authorised activity, its duration and the regularity of reviews. A record should be made of such comments and of the action taken by the Authorising Officer to incorporate or address them.

294. An authorisation of directed surveillance or CHIS does not take effect until it has been approved and signed by the magistrate. Local authorities should record the dates and times of signature by both the Authorising Officer and the magistrate. Care should be taken to record the expiry date accurately thereafter (see Notes 87 and 135).

295. Local authorities in England and Wales should also bear in mind that the power to make urgent oral authorisations has been removed, because section 43(1)(a) of RIPA no longer applies to authorisations requiring a magistrate's approval. All authorisations, even if urgent, must be made in writing, and local authorities' RIPA policy documents should make this clear.
[70]

Appendix 1A

Senior Responsible Officer, RIPA Coordinator and Authorised and Designated Officer

The Councils Lead officer on RIPA (Senior Responsible Officer) is the Strategic Director of Corporate Resources (Joanne Hyde) who works in consultation with the Councils RIPA coordinator.

This position was created is in response to Home Office Guidance and Regulation published in winter 2009 and spring 2010 to take effect in April 2010.

In accordance with Regulations coming in force on the 6th April 2010 she is the senior Responsible Officer (SRO) for RIPA.

The appointed RIPA Coordinator and Monitoring officer for the Council for the purposes of the Regulation of Investigatory Powers Act 2000 is Jason Field – Head of Legal.

The Councils RIPA coordinator is also the Councils Single Point of Contact for the purpose of Part 1 Chapter2 (access to communications data) of RIPA having attended the Home offices accredited course in September 2004.

Officer:	**Department:**	**Contact Details:**
Jason Field Head of Legal	Legal Services	Tel: 07890 416571 Jason.fieldr@bradford.gov.uk

Authorised and Designated Officer

The following Officers are Authorised Officers for the specified purpose on behalf of City of Bradford Metropolitan District Council under the Regulation of Investigatory Powers Act 2000 and associated regulations and codes of practice. Directorates not listed below should contact the Councils RIPA Coordinator for guidance.

The Head of the Councils Paid Service i.e. the Councils Chief Executive is the only officer of the Council authorised to grant an authorisation which is likely to lead to the acquisition of confidential and religious information see pages 13 and 14.

Extent of Authorisation for Investigations within the office of the Chief Executive and relevant Departments:	Designated/Authorising officer:	Approval to Authorise:		
		Communications Data	DCS CHIS	Confidential Material:
The Chief Executive Office	Chief Executive.	No	No	yes
Department of Place:	Assistant Director-	No	No	No
Development Control	Director of Legal and Governance	Yes	Yes	No
Private sector Housing	Director of Legal and Governance	yes	Yes	No
		Yes	Yes	No
Taxi Licensing Enf.)	Director of Legal and Governance	Yes	Yes	No
Environmental Health	Director of Legal and Governance	Yes	Yes	No
Licensing (Licensing Act 2003 Enforcement)	Director of Legal and Governance	Yes	Yes	No
Adult social care and Children's services	Director of Legal and Governance	yes	yes	No
Corporate Resources	Assistant Director	Yes	Yes	No
Revenues and Benefits	Director of Legal and Governance	Yes	Yes	No
Counter Fraud Team	Director of Legal and Governance	Yes	Yes	No
Internal Audit	Director of Legal and Governance	Yes	Yes	No
Legal Services-	Director of Legal and Governance	Yes	yes	No

NB1: In all Council Departments whether or not listed above the Officer must be of a rank of at least assistant chief officer i.e. Director Head of Service or Service Manager or

equivalent see SI 2010 571. There is no provision for officers of a lower rank to authorise DCS, CHIS or ACD.

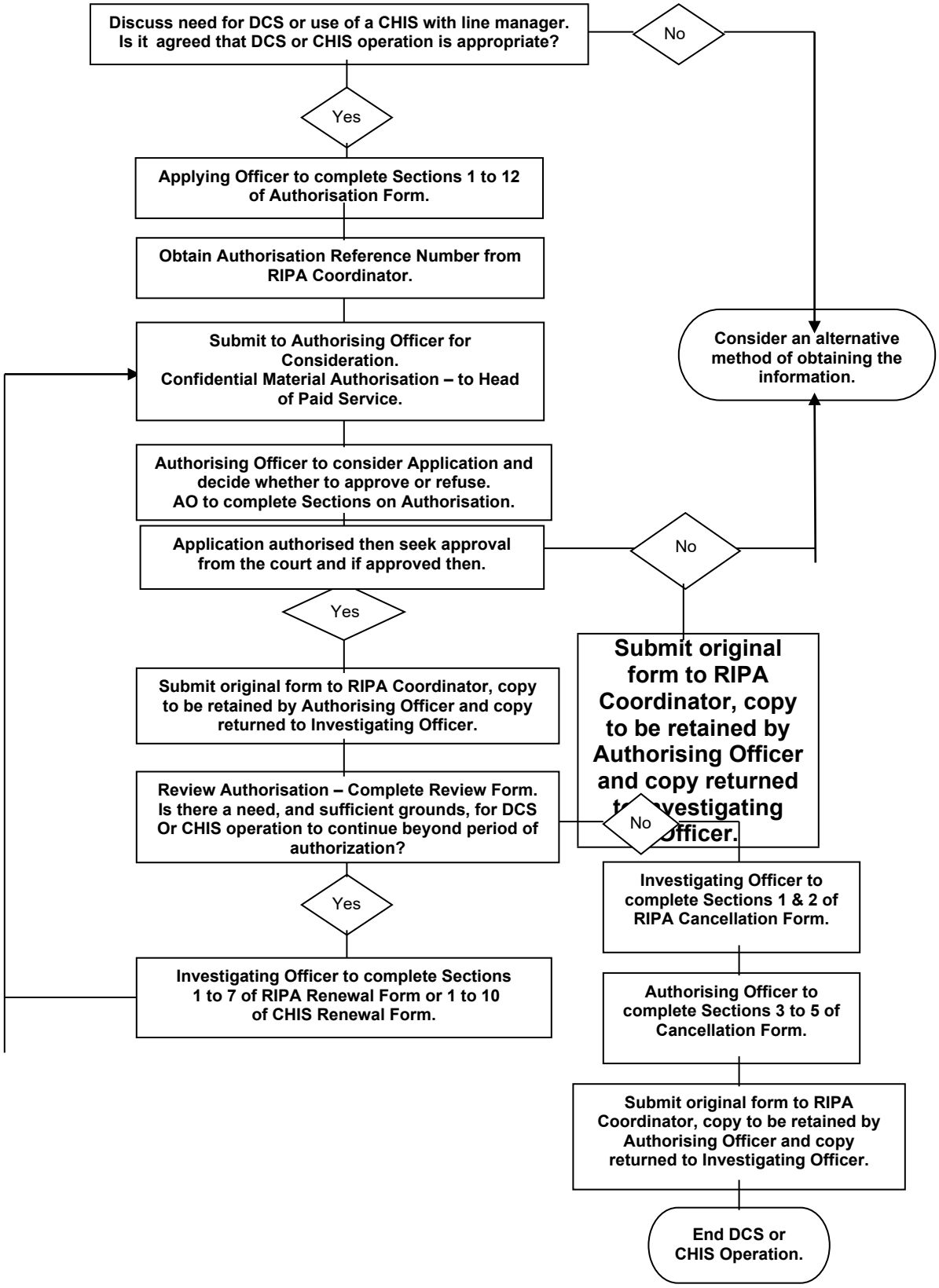
NB1 Only the Councils Head of Paid service ie Chief Executive can authorise investigations that will involve the collection of confidential material.
NB2 Since 2011 There are two authorised officers who are the Councils Chief Executive, and Director of Legal and Governance in consultation with the Leader of Council.
NB3 Their deputies can also authorise in their absence as approved by Committee on the 4th April 2014

Appendix 2

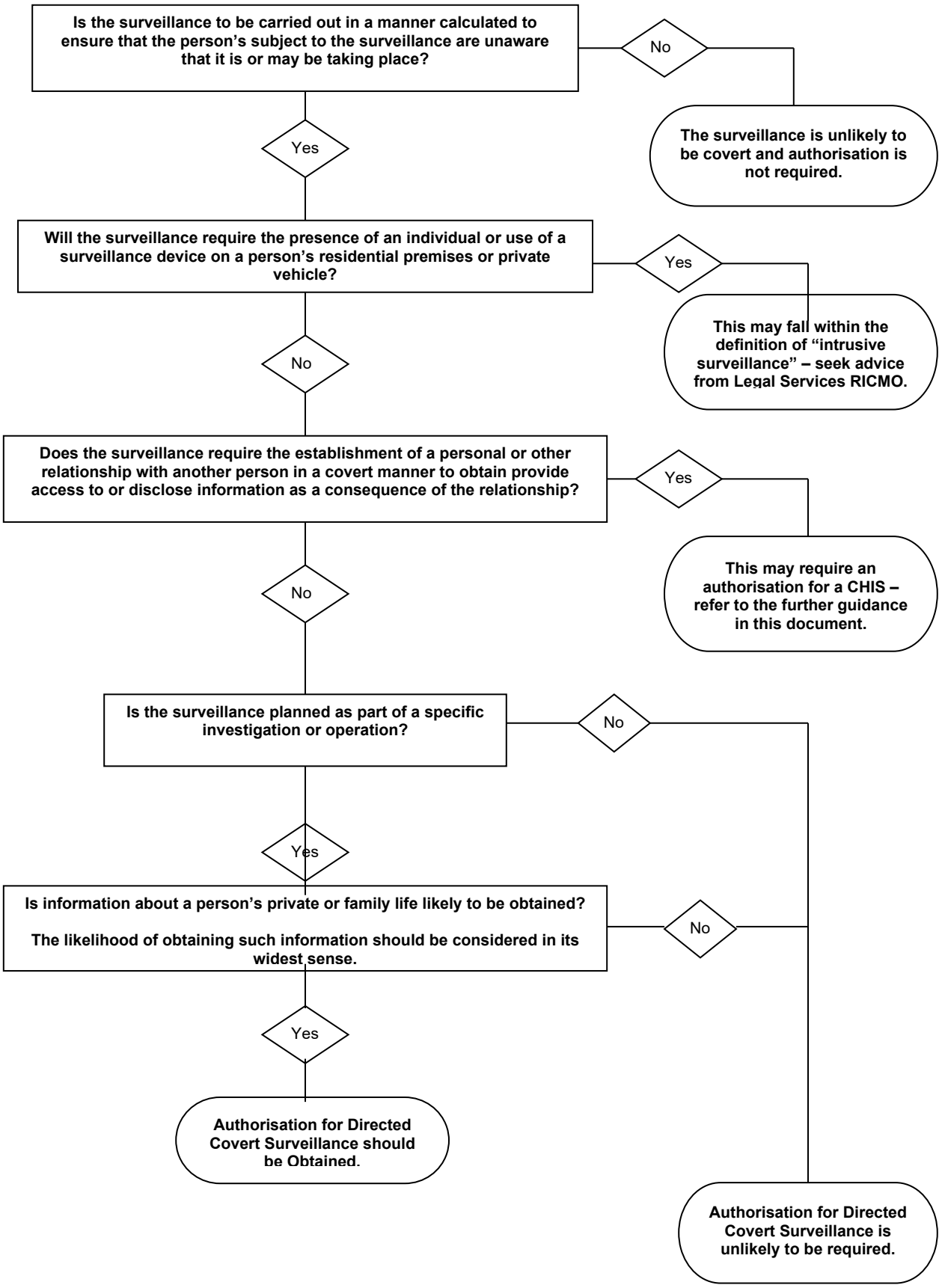
Flowcharts

1. RIPA Procedure.
2. DCS Authorisation.
3. CHIS Authorisation.
4. Access to Tele-Communications Data (ACoD)

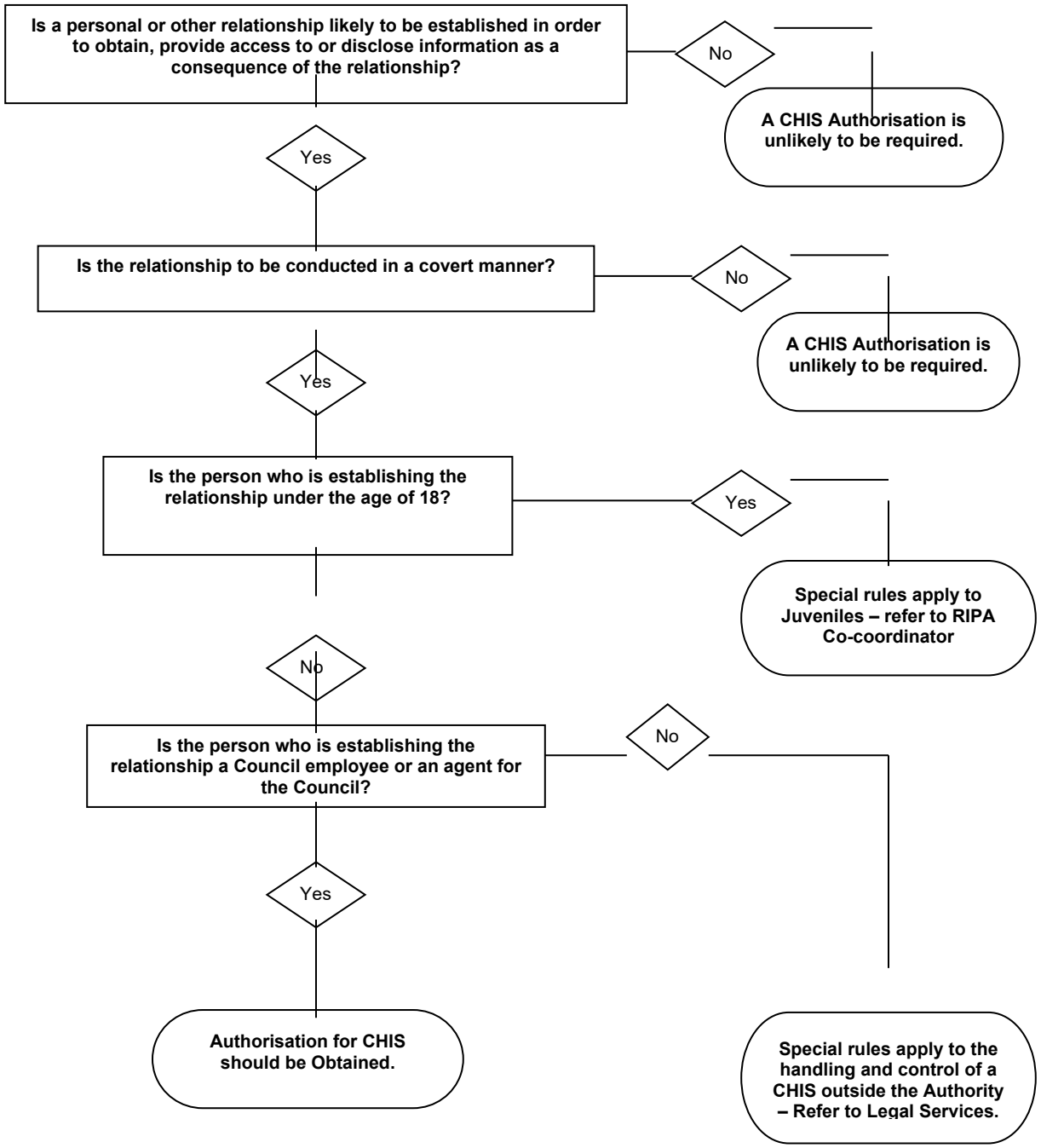
Procedure for Obtaining RIPA Authorisation and court approval



Determination of Whether DCS Authorisation and court approval is required



Determination of Whether CHIS Authorisation and court approval is required



Appendix 3

RIPA Forms

RIP1 Application for Authorisation for DCS (Guidance document and blank form).

RIP2 Review Form for DCS

RIP3 Application to Renew Authorisation for DCS (blank form).

RIP4 Application to Cancel Authorisation for DCS (blank form).

RIP5 Application for Authorisation for CHIS (blank form).

RIP6 Review Form for CHIS

RIP7 Application to Renew Authorisation for CHIS (blank form).

RIP8 Application to Cancel Authorisation for CHIS (blank form).

RIP9 Application for authorisation to obtain communications data (ACoD) (guidance documents and blank form)

RIP 1

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance last update November 2012

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 571 ; [4] Director, Head of Service, Service Manager or equivalent
2. Describe the purpose of the specific operation or investigation. *The serious offence test must be satisfied before an application can be authorised ie the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)*
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, and recorder) that may be used.

[4] For local authorities: The exact position of the authorising officer should be given. For example, Head of Audit Service.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

5. Explain the information that it is desired to obtain as a result of the directed surveillance. ***The serious offence test must be satisfied before an application can be authorised ie the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)***

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (SI 2010 No.571****) The serious offence test must be satisfied before an application can be authorised ie the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)***

- For the purpose of preventing or detecting crime or of preventing disorder;

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3-3.4]

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8-3.11]

Describe precautions you will take to minimise collateral intrusion

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Covert Surveillance and Property Interference Revised Code 2010 (paragraph 3.5-3,7]
10. Confidential information. [Revised 2010 Code paragraphs 4.1-4.15] INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details.			
Name (print)		**Tel No:**	
Grade/Rank		Date	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; what; Where; When; Why and HOW– in this and the following box.]

NB The authorisation set out below cannot be acted upon by the Councils investigators until the authorisation has been approved by the magistrates Court. RIPA 2000 as amended by the Protection of Freedoms Act 2012

I hereby authorise directed surveillance defined as follows:

13. Explain why you believe the directed surveillance is necessary. [2010 revised Code paragraph 3.3-.3. 4]

Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Revised 2010 Code paragraphs 3.5-3.7]

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1- 4.15

Date of first review	

Programmed for subsequent reviews of this authorisation: [2010 revision to Code Chapter 5]. Only complete this box if review dates after first review is known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		**Grade / Rank**		
Signature		**Date and time**		

Expiry date and time [e.g.: authorisation granted on 1 April 2010 - expires on 30 June 2010, 23.59]	

15. Urgent Authorisation [2010 Code paragraphs 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer

Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		

Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

RIP 1 GUIDANCE

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance last update November 2012

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

DETAILS OF APPLICATION

1. **Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 571; For Local authorities i.e. Director Head of Service Manager or Equivalent (enter name and rank/position below)**

2. **Describe the purpose of the specific operation or investigation.** ***The serious offence test must be satisfied before an application can be authorised ie the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)***

WHAT INFORMATION CAN BE OBTAINED FROM THE RESULTING AUTHORISATION TO PROVE OR DISPROVE THE ALLEGED OFFENCE

(THE INFORMATION RECORDED MUST BE OBJECTIVE AND NOT INDICATE A PRESUMPTION OF GUILT TOWARDS THE CUSTOMER(S).

WORDING SUCH AS "IN ORDER TO PROVE MR X HAS COMMITTED xxxxxx OFFENCE", **WOULD SHOW THAT THE INVESTIGATION IS NOT BEING CARRIED OUT IMPARTIALLY AND THEREFORE NOT WITHIN THE SPIRIT OF THE ACT.)**

3. **Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, and recorder) that may be used.**

RECORD IN THIS BOX:

a) THE TYPE/METHOD OF SURVEILLANCE TO BE UNDERTAKEN E.G. static, mobile,

b) HOW SURVEILLANCE WILL BE CONDUCTED E.G. still camera, video camera, visual obs with notes taken, test purchasing, CCTV, recording of telephone conversations etc

c) THE LOCATION(S) WHERE SURVEILLANCE WILL TAKE PLACE E.G. IF SURVEILLANCE IS TO TAKE PLACE IN A POST OFFICE, STATE WHICH POST OFFICE

d) HOW WILL THE NUMBER OF OFFICERS MENTIONED IN BOX 2(b) BE DEPLOYED AT ANY ONE TIME FOR THE TYPE(S) OF SURVEILLANCE TO BE UNDERTAKEN

4. **The identities, where known, of those to be subject of the directed surveillance.**

- Name:
- Address:
- DOB:
- Other information as appropriate:

ENTRY: RECORD DETAILS OF **ALL** SUBJECTS OF SURVEILLANCE. IF SUBJECT NAME IS NOT KNOWN, NOTE WHETHER "MALE/FEMALE" AND DESCRIPTION, IF KNOWN.

5. Explain the information that it is desired to obtain as a result of the directed surveillance. ***The serious offence test must be satisfied before an application can be authorised ie the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)***

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (SI 2010 no 571)* ***The serious offence test must be satisfied before an application can be authorised i.e. the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)***

- For the purpose of preventing or detecting crime or of preventing disorder;

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3-3.4]

RECORD IN THIS BOX:

a) SUMMARY OF THE CASE (INCLUDE DETAILS OF THE ALLEGATION)
b) WHAT OPTIONS OTHER THAN SURVEILLANCE HAVE BEEN CONSIDERED/USED AND THE OUTCOME OF THOSE OPTIONS
c) WHY COVERT SURVEILLANCE IS THE ONLY OPTION

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8-3.11.]

Describe precautions you will take to minimise collateral intrusion

RECORD:

a) WHETHER SURVEILLANCE WILL INTRUDE INTO A THIRD PARTY'S PRIVACY I.E. SOMEONE OTHER THAN THE SUBJECT(S) OF SURVEILLANCE. EXAMPLES ARE: -

- ❑ MEMBERS OF THE PUBLIC IN THE SURVEILLANCE AREA.
- ❑ WORK COLLEAGUES OF THE SUBJECT(S)
- ❑ NEIGHBOURS
- ❑ CHILDREN OF THE SUBJECT(S) - INCLUDE, IF KNOWN, THEIR DATES OF BIRTH
- ❑ OTHERS KNOWN TO BE IN THE HOUSEHOLD - INCLUDE, IF KNOWN, THEIR DATES OF BIRTH

(THIS LIST IS NOT EXHAUSTIVE)

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 3.5-3.7]

RECORD IN THIS BOX:

a) THE LENGTH OF TIME REQUIRED FOR SURVEILLANCE

b) HOW MANY OFFICERS WILL DEPLOYED AT ANY ONE TIME?

c) ANY INFORMATION ABOUT THE SUBJECTS NORMAL ROUTINE IN RELATION TO THE ALLEGED OFFENCE

10. Confidential information. [Code paragraphs 4.1-4.15]

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

IT IS UNLIKELY THAT CONFIDENTIAL INFORMATION WILL BE OBTAINED IN THE COURSE AN INVESTIGATION.

CONFIDENTIAL INFORMATION CONSISTS OF:

- "MATTERS SUBJECT TO LEGAL PRIVILEGE"
- "CONFIDENTIAL PERSONAL INFORMATION"
- "CONFIDENTIAL JOURNALISTIC MATERIAL"

11. **Applicant's Details**.			
Name (print)		**Tel No:**	
Grade/Rank		Date	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; what; Where; When; Why and HOW– in this and the following box.]

NB The authorisation set out below cannot be acted upon by the Council investigators until the authorisation has been approved by the magistrates Court. RIPA 2000 as amended by the Protection of Freedoms Act 2012

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, against whom is the surveillance directed against, Where and When will it take place, what surveillance activity/equipment is sanctioned, how is it to be achieved?]*

*This written authorisation will cease to have effect at the end of a period of 3 months unless renewed.
(*delete where authorisation is refused.)
This authorisation will be reviewed frequently to assess the need for authorisation to continue.

ENTRY: THE AUTHORISING OFFICER STATEMENT SHOULD REFLECT THAT INDIVIDUAL CONSIDERATION HAS BEEN GIVEN TO THE REQUEST FOR SURVEILLANCE, TAKING INTO ACCOUNT THE NECESSITY, PROPORTIONALITY AND APPROPRIATENESS OF IT. **STANDARD WORDING SHOULD NOT BE USED.**

- CONSIDER THE INFORMATION PROVIDED IN BOXES 2-7 OF THE RIP 1
- IF THE CASE HAS BEEN DISCUSSED WITH THE APPLICANT/LINEMANAGER, RECORD THE DETAILS
- RECORD IF OPTIONS OTHER THAN SURVEILLANCE ARE APPROPRIATE AND WHY
- RECORD IF THE PROPOSED SURVEILLANCE IS A REASONABLE MEANS OF ACHIEVING THE DESIRED RESULT
- RECORD WHETHER SURVEILLANCE IS EXCESSIVE IN RELATION TO THE INVESTIGATION/TYPE OF BENEFIT FRAUD
- SPECIFY THE COVERT SURVEILLANCE ACTIVITY BEING AUTHORISED

Extract from OSC Guidance December 2010

Necessity

104 The authorising officer must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in s28 (3) of RIPA and s.29 (3) of RIP(S) A. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. Often missed is an explanation of why it is necessary to use the covert techniques requested.

Proportionality

105 Proportionality is a key concept of RIPA and RIP(S) A. It is often poorly articulated. An authorisation should demonstrate how an authorising officer had reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

106 A potential model answer would make clear that the four elements of proportionality had been fully considered:

106.1 balancing the size and scope of the operation against the gravity and extent of the perceived mischief,

106.2 explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,

106.3 that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and

106.4 providing evidence of other methods considered and why they were not implements.

"I am satisfied" and "I believe"

107 The authorising officer should set out, in his own words, why he is satisfied (RIP(S) A) or why he believes (RIPA) the activity is necessary and proportionate. A bare assertion is insufficient.

****

13. **Explain <u>why</u> you believe the directed surveillance is necessary. [Code paragraph 3.3-3.4]**

Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 3.5-3.7]

14. **(Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.15**

Date of first review	

Programmed for subsequent reviews of this authorisation: [Code chapter 5]. Only complete this box if review dates after first review is known. If not or inappropriate to set additional review dates then leave blank.

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

15. Urgent Authorisation [Code paragraphs 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

IS URGENT SURVEILLANCE NECESSARY TO ESTABLISH PERTINENT FACTS?
IF SO, WHY? (urgent applications must only be used sparingly)

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer

IS URGENT SURVEILLANCE NECESSARY TO ESTABLISH PERTINENT FACTS?
IF SO, WHY?

Name (Print)		**Grade/**		

		Rank		
Signature		**Date and Time**		

Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation Last Update November 2012

Public Authority *(including address)*	

Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** ***Filing Ref**	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	Date

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicant's Details

Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.

I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal] [it should be cancelled immediately].

Name (Print)	.....	**Grade / Rank**	- - - - - - - - - - - - - - - - - - - -
Signature	- - - - - - - - - - - - - - - - -	**Date**	- - - - - - - - - - - - - - - - - - - -

10. Date of next review.	

RIP3 Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation- Last Update November 2012

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	Date

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the results of the regular reviews of the investigation or operation.

7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Authorising Officer's Comments. **This box must be completed.**

9. Authorising Officer's Statement.
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.

Name (Print)	----------	**Grade / Rank**	----------
Signature	------ ------ ----	**Date**	---------- --
Renewal From: **Time:**		**Date:**	

Date of first review.	
Date of subsequent reviews of this authorisation.	

RIP 4 Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorization (GUIDANCE DOCUMENT)
Last Update November 2012

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:
GIVE FULL EXPLANATION AS TO WHY IT IS NO LONGER NECESSARY TO CONTINUE SURVEILLANCE. EXAMPLES ARE: • OBJECTIVE(S) ESTABLISHED? IF NOT, WHY? • OBJECTIVE(S) ACHIEVED BY MEANS OTHER THAN SURVEILLANCE? • SUBJECT(S) NO LONGER PART OF INVESTIGATION? **(THIS LIST IS NOT EXHAUSTIVE)**

2. Explain the value of surveillance in the operation:
WHAT WAS ACHIEVED AS A RESULT OF THE AUTHORISATION FOR SURVEILLANCE, WITH REFERENCE TO BOX 5 OF THE RIP 1 OR BOX 3 OF THE RIP 2? (If there has been no value to the surveillance, explain why.)

3. Authorising officer's statement.			
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	.....	**Grade**	.....
Signature	.....	**Date**	.....

4. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled.	**Date:**	**Time:**

RIP4 (BLANK)

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation-last update November 2012

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

6. Explain the reason(s) for the cancellation of the authorisation:

7. Explain the value of surveillance in the operation:

8. Authorising officer's statement.			
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	----------	**Grade**	----------
Signature	----------	**Date**	----------

9. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

10.Authorisation cancelled.	**Date:**	**Time:**

RIP5

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS) (see 2010 code for guidance

Last Update November 2012

Public Authority *(including full address)*	

Name of Applicant		**Service/Department/Branch**	
How will the source be referred to? i.e. what will be his/her pseudonym or reference number			
The name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare. (Often referred to as the Handler)			
The name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source. (Often referred to as the Controller)			

Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source's true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?	
Investigation/Operation Name (if applicable)	

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 no 571. [5] *Where appropriate throughout amend references to the Order relevant to your authority i.e. in local government -Director Head of Service Manager or equivalent*
2. Describe the purpose of the specific operation or investigation. *The serious offence test must be satisfied before an application can be authorised i.e. the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)*

[5] For local authorities: The formal position of the authorising officer should be given. For example, Head of Audi Service.

3. Describe in detail <u>the purpose</u> for which the source will be tasked or used.
4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.
5. <u>Identify on which grounds the conduct or the use of the source is necessary</u> under Section 29(3) of RIPA. *<u>Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (E.g. SI 2010 No 5711</u>**<u>) The serious offence test must be satisfied before an application can be authorised i.e. the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)</u>***
• For the purpose of preventing or detecting crime or of preventing disorder;

6. Explain why this conduct or use of the source is necessary on the grounds you have identified [see Code]
7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code.] Describe precautions you will take to minimise collateral intrusion and how any will be managed.
8. Is there any particular sensitivity in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source? (see Code)

9. Provide an assessment of the risk to the source in carrying out the proposed conduct. (see Code 2010)
10. Explain <u>why</u> this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means? [Code paragraph]
11. Confidential information. [see Code] **Indicate the likelihood of acquiring any confidential information.**
References for any other linked authorisations:
12. Applicant's Details.

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

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.
NB The Councils investigators cannot act upon the authorisation below until it has been approved by the Magistrates Court.
14. Explain why you believe the conduct or use of the source is necessary. [Code paragraph 2.4] **Explain why you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement. [see Code]**
15. (Confidential Information Authorisation.) Supply details demonstrating compliance with see Code

16. Date of first review:	

17. Programmed for subsequent reviews of this authorisation: [see Code]. Only complete this box if review dates after first review is known. If not, or inappropriate to set additional review dates, and then leave blank.

18. Authorising Officer's Details			
Name (Print)		**Grade/Rank/Position**	
Signature		Time and date granted* Time and date authorisation ends	

**** Remember, an authorisation must be granted for a 12-month period, i.e. 1700 hrs 4th June 2006 to 2359hrs 3 June 2007***

19. Urgent Authorisation [see Code]: Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer

21. Authorising Officer of urgent authorisation				
Name (Print)		**Grade/Rank/Position**		
Signature		**Date and Time**		
Urgent authorisation expiry date:		**Expiry time:**		
Remember the 72-hour rule for urgent authorisations – check Code of Practice [Code2010]. e.g. authorisation granted at 1700 on 1st June 2006 expires 1659 on 4th June 2006				

RIP6

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000
Cancellation of an authorisation for the use or conduct of a Covert Human Intelligence Source Last update September 2010

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of the source in the operation:

3. Authorising officer's statement. THIS SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.			
Name (Print)	----------	**Grade**	----------
Signature	----------	**Date**	----------

4. Time and Date of when the authorising officer instructed the use of the source to cease.			
Date:		**Time:**	

RIP7
Part II of the Regulation of Investigatory Powers Act (RIPA) 2000Last Update November 2012

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation

(Please attach the original authorisation)

Public Authority *(including full address)*	

Name of Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	Date

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail why it is necessary to continue with the authorisation, including details of any tasking given to the source.

4. Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.

5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.

6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source.

7. Detail the results of regular reviews of the use of the source.

8. Give details of the review of the risk assessment on the security and welfare of using the source.

9. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

10. Authorising Officer's Comments. <u>This box must be completed.</u>

11. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE

PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

Name (Print)	----------	**Grade / Rank**
Signature		**Date**
Renewal From:	**Time:**	**Date:** **End date/time of the authorisation**

NB. Renewal takes effect at the time/date of the original authorisation would have ceased but for the renewal

Date of first review:	
Date of subsequent reviews of this authorisation:	

RIP8

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Review of a Covert Human Intelligence Source (CHIS) authorization Last Update November 2012

Public Authority *(including full address)*	

Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Operation Name		**Operation Number*** ***Filing Ref**	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	Date

2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue with using a Covert Human Intelligence Source.

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Give details of the review of the risk assessment on the security and welfare of using the source.

8. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

9. Review Officer's Comments, including whether or not the use or conduct of the source should continue?

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

Name (Print)	----------	**Grade / Rank**	
Signature		**Date**	

Date of next review:	

RIP9

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA)

Application for Communications Data

This form is to obtain authorisation to issue a RIPA Section 22 Notice to a CSP to release Communications Data

Last Update November 2012

Name of Public Authority making this application:

_____

1) Applicant's Name		**4) Unique Reference Number**	
2) Office, Rank or Position		**5) Applicant's Telephone Number.**	
3) Applicant's Email Address		**6) Applicant's Fax Number**	

7) Operation Name (if applicable)		**8) STATUTORY PURPOSE** ***The serious offence test must be satisfied before an application can be authorised i.e. the offence(s) been investigated carry a penalty of imprisonment of six months or more. RIPA 2000 as amended by the Protection of Freedoms Act 2012 (1st November 2012)***
		For the purpose of the prevention or detection of crime

9) COMMUNICATIONS DATA **Describe the communications data, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)**

10) NECESSITY **State why it is necessary in relation to your investigation or operation to obtain this data for the purpose listed at question 8)** *What do you expect to achieve from obtaining the communications data? Explain why you have requested the specific date/time period. If applicable, explain the time scale within which the data is required to be delivered to you.*

11) PROPORTIONALITY **State why obtaining the communications data is proportionate to what you are seeking to achieve** *Why does the intrusion benefit the investigation or operation you are undertaking? When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy?*

12) COLLATERAL INTRUSION **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** *If you have identified any meaningful degree of collateral intrusion, explain what it is.*

13) TIMESCALE **Identify and explain the timescale within which the data is required**	

14) APPLICANT **I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data**			
Applicant's Signature		**Date**	

15) ASSESSMENT BY ACCREDITED SPoC.	
If the request is NOT reasonably practical for	

the CSP explain why	
Specify which sub-section the data falls within	*Click here for options:-*
State whether notice or authorisation is appropriate	*Click here for options:-*
Describe any adverse cost or resource implications to either your public authority or the CSP?	
If the request will provide any excessive data to that requested by the applicant, give details.	
Are there other factors the DP should be aware of?	
Name of Accredited SPoC	

16) AUTHORISATION (Completed by Accredited SPoC when appropriate)

Specify the reason why the collection of communications data by means of an authorisation is appropriate:

☐ CSP is not capable of obtaining or disclosing the communications data;

☐ The investigation or operation may be prejudiced if the CSP is required to obtain or disclose the data;

☐ There is an agreement in place between the public authority and the CSP relating to the appropriate

mechanisms for the disclosure of the data;

☐ The designated person considers there is a requirement to conduct a telephone subscriber check but a CSP

Has yet to be conclusively determined as the holder of the communications data.

Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought. Also, describe the course of conduct required to obtain it.	
Name of the relevant CSP	

The statutory purpose for which the conduct may be authorised is set out at section 8 of this form.

The office, rank or position of the designated person should be recorded within section 17 of this form.

A record of the date & time the granting of an authorisation is made should be recorded within section 17 of this form

17. DESIGNATED PERSON			
The Designated Person considers the application and if approved records their considerations: *If you, based on this application,* ***believe*** *acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act consider the following;* • *Why do you* ***believe*** *the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgment you should take in consideration any additional information from the SPoC.* • *Where accessing the communication data is likely to result in meaningful degree of collateral intrusion, why you* ***believe*** *the request remains justified and proportionate to the objective(s)?*			
My considerations in approving / not approving this application are:			
☐ I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form. ☐ I give Notice and require the SPoC to serve it on (insert name of CSP) . The Notice bears the unique reference number			
Name		***Office, Rank or Position***	
Signature		**Time and Date**	

CHAPTER II

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

Lawful acquisition and disclosure of communications data.

21. - (1) This Chapter applies to-

(a) any conduct in relation to a postal service or telecommunication system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system; and

(b) the disclosure to any person of communications data.

(2) Conduct to which this Chapter applies shall be lawful for all purposes if-

(a) it is conduct in which any person is authorised or required to engage by an authorisation or notice granted or given under this Chapter; and

(b) the conduct is in accordance with, or in pursuance of, the authorisation or requirement.

(3) A person shall not be subject to any civil liability in respect of any conduct of his which-

(a) is incidental to any conduct that is lawful by virtue of subsection (2); and

(b) is not itself conduct an authorisation or warrant for which is capable of being granted under a relevant enactment and might reasonably have been expected to have been sought in the case in question.

(4) In this Chapter "communications data" means any of the following-

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person-

(i) of any postal service or telecommunications

service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

(5) In this section "relevant enactment" means-

(a) an enactment contained in this Act;

(b) section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services); or

(c) an enactment contained in Part III of the Police Act 1997 (powers of the police and of customs officers).

(6) In this section "traffic data", in relation to any communication, means-

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,

(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,

(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication,

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

(7) In this section-

(a) references, in relation to traffic data comprising signals for the actuation of apparatus, to a telecommunication system by means of which a communication is being or may be transmitted include references to any telecommunication system in which that apparatus is comprised; and

(b) references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other;

and in this section "data", in relation to a postal item, means

anything written on the outside of the item.

Obtaining and disclosing communications data.

22. - (1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.

(2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary-

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

(3) Subject to subsection (5), the designated person may grant an authorisation for persons holding offices, ranks or positions with the same relevant public authority as the designated person to engage in any conduct to which this Chapter applies.

(4) Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator-

(a) if the operator is not already in possession of the data, to obtain the data; and

(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

(5) The designated person shall not grant an authorisation under subsection (3), or give a notice under subsection (4), unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining

the data.

(6) It shall be the duty of the postal or telecommunications operator to comply with the requirements of any notice given to him under subsection (4).

(7) A person who is under a duty by virtue of subsection (6) shall not be required to do anything in pursuance of that duty which it is not reasonably practicable for him to do.

(8) The duty imposed by subsection (6) shall be enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(9) The Secretary of State shall not make an order under subsection (2) (h) unless a draft of the order has been laid before Parliament and approved by a resolution of each House.

Form and duration of authorisations and notices.

23. - (1) An authorisation under section 22(3)-

(a) must be granted in writing or (if not in writing) in a manner that produces a record of its having been granted;

(b) must describe the conduct to which this Chapter applies that is authorised and the communications data in relation to which it is authorised;

(c) must specify the matters falling within section 22(2) by reference to which it is granted; and

(d) must specify the office, rank or position held by the person granting the authorisation.

(2) A notice under section 22(4) requiring communications data to be disclosed or to be obtained and disclosed-

(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;

(b) must describe the communications data to be obtained or disclosed under the notice;

(c) must specify the matters falling within section 22(2) by reference to which the notice is given;

(d) must specify the office, rank or position held by the person giving it; and

(e) must specify the manner in which any disclosure required by the notice is to be made.

(3) A notice under section 22(4) shall not require the disclosure of data to any person other than-

(a) the person giving the notice; or

(b) such other person as may be specified in or otherwise identified by, or in accordance with, the provisions of the notice;

but the provisions of the notice shall not specify or otherwise identify a person for the purposes of paragraph (b) unless he holds an office, rank or position with the same relevant public authority as the person giving the notice.

(4) An authorisation under section 22(3) or notice under section 22(4)-

(a) shall not authorise or require any data to be obtained after the end of the period of one month beginning with the date on which the authorisation is granted or the notice given; and

(b) in the case of a notice, shall not authorise or require any disclosure after the end of that period of any data not in the possession of, or obtained by, the postal or telecommunications operator at a time during that period.

(5) An authorisation under section 22(3) or notice under section 22(4) may be renewed at any time before the end of the period of one month applying (in accordance with subsection (4) or subsection (7)) to that authorisation or notice.

(6) A renewal of an authorisation under section 22(3) or of a notice under section 22(4) shall be by the grant or giving, in accordance with this section, of a further authorisation or notice.

(7) Subsection (4) shall have effect in relation to a renewed authorisation or renewal notice as if the period of one month mentioned in that subsection did not begin until the end of the period of one month applicable to the authorisation or notice that is current at the time of the renewal.

(8) Where a person who has given a notice under subsection (4) of section 22 is satisfied-

(a) that it is no longer necessary on grounds falling within subsection (2) of that section for the requirements of the notice to be complied with, or

(b) that the conduct required by the notice is no longer proportionate to what is sought to be achieved by obtaining communications data to which the notice relates,

he shall cancel the notice.

(9) The Secretary of State may by regulations provide for the person by whom any duty imposed by subsection (8) is to be performed in a case in which it would otherwise fall on a person who is no longer available to perform it; and regulations under this subsection may provide for the person on whom the duty is to fall to be a person appointed in accordance with the regulations.

Arrangements for payments.

24. - (1) It shall be the duty of the Secretary of State to ensure that such arrangements are in force as he thinks appropriate for requiring or authorising, in such cases as he thinks fit, the making to postal and telecommunications operators of appropriate contributions towards the costs incurred by them in complying with notices under section 22(4).

(2) For the purpose of complying with his duty under this section, the Secretary of State may make arrangements for payments to be made out of money provided by Parliament.

Interpretation of Chapter II.

25. - (1) In this Chapter-

"communications data" has the meaning given by section 21(4);

"designated" shall be construed in accordance with subsection (2);

"postal or telecommunications operator" means a person who provides a postal service or telecommunications service;

"relevant public authority" means (subject to subsection (4)) any of the following-

(a) a police force;

(b) the National Criminal Intelligence Service;

(c) the National Crime Squad;

(d) the Commissioners of Customs and Excise;

(e) the Commissioners of Inland Revenue;

(f) any of the intelligence services;

(g) any such public authority not falling within paragraphs (a) to (f) as may be specified for the purposes of this subsection by an order made by the Secretary of State.

(2) Subject to subsection (3), the persons designated for the purposes of this Chapter are the individuals holding such offices, ranks or positions with relevant public authorities as are prescribed for the purposes of this subsection by an order made by the Secretary of State.

(3) The Secretary of State may by order impose restrictions-

(a) on the authorisations and notices under this Chapter that may be granted or given by any individual holding an office, rank or position with a specified public authority; and

(b) on the circumstances in which, or the purposes for which, such authorisations may be granted or notices given by any such individual.

(4) The Secretary of State may by order remove any person from the list of persons who are for the time being relevant public authorities for the purposes of this Chapter.

(5) The Secretary of State shall not make an order under this section that adds any person to the list of persons who are for the time being relevant public authorities for the purposes of this Chapter unless a draft of the order has been laid before Parliament and approved by a resolution of each House.

Appendix 4

Scenarios

The following is intended as a guide only and any interpretation of how the Act is, or is not, being properly implemented is ultimately a matter for the Courts.

Q. I receive a complaint from a member of the public about anti social behaviour/fly tipping/other nuisance activity. I ask them to keep a diary of events to confirm their complaint. Does the resident need to be authorised as a CHIS or the surveillance as DS?

A. The person is not being asked to enter into a covert relationship with any individual and therefore authorisation for CHIS is not required. Likewise, when complainants are merely confirming their complaints by using a diary a DS authorisation is not required. However, if you invite them to use a camera recording events in a street or garden

then a DS authorisation would be required. If previously collected video recordings are volunteered, then no DS is required. If you ask a private detective to collect information then a DS would always be required.

Q. I want to install a tape recorder in a complainant's property to record the noise coming from a neighbouring property. Do I need a DS authorisation?

A. If the neighbour, or any other person attending that property, was unaware that surveillance was being undertaken then a DS authorisation would be required.

Q. I am undertaking noise monitoring using a sound level meter. Do I need a DS authorisation?

A. It depends on what the noise source is. If the noise is not coming from the activity of a person (e.g. machinery, entertainment venue, traffic etc) then a DS authorisation would not be required. Even if the monitoring related to noise from the activity of an individual (domestic behaviour etc), and the subject was unaware that the monitoring was to take place a DS authorisation would still not be required as the data held on the sound level meter in terms if decibel readings would not be considered as private information, but as the Officer controlling the machine would hear activity then a DS in these circumstances would be required.

Q. I need to use a pair of binoculars to be able to observe the activity of premises which has been the subject of a complaint. Do I need a DS authorisation?

A. The use of the binoculars (or other such device which enhances sensory perception) does not in itself mean a DS authorisation is required. The test is whether the covert surveillance is targeted towards an individual person which may result in private information being obtained about that individual.

Q. I have reason to believe that a milkman is employing a 13yr old in the early morning, I want to follow the milk delivery to establish this, and do I need any authorisation?

A. Yes, you need a DS as you are likely to gather private information. You will also need to consider collateral intrusion in respect of others employed by the milkman.

Q. I need to visit a factory to see if the owner has removed an unauthorised extension in compliance with a Planning Enforcement Notice. Does this need a DS authorisation?

A. No you are not likely to obtain private information, you are observing a structure. In any event in such circumstances you will have told the owner of your activity therefore your surveillance would be overt.

Q. I want to place a hidden camera to observe a cashier as part of a suspected internal fraud investigation, do I need authorisation and would the answer be different if no camera was used.

A. You need a DS authorisation whether video is used or not. The consideration is not whether the use of the video needs authorising, it is the subject and purpose of the investigation that matters.

Q. I wish to install a covert camera on a garage site to find out who is dumping cars and setting fire to them, does this need authorisation?

A. Yes, a DS, but the authorising officer would have to consider collateral intrusion and proportionality of the matter very carefully as the site is likely to be used by a number of people for legitimate purposes.

Q Do I need an authorisation to make a test purchase of food in order to establish whether the product confirms to the relevant food standard?

A If the test purchaser, simply pays for the goods he has requested he would not be acting as a CHIS and would not require authorisation. This is because the test purchaser is not establishing or maintaining a personal or other relationship nor is he obtaining any information which would be considered to be a breach of Article 8. If, however the test purchaser has a verbal exchange beyond merely requesting and paying for the goods and obtains any information about the business or trader he would be acting as a CHIS and would need an authorisation. Consideration should also be given to the obtaining of a DS authorisation if another Council Enforcement Officer is in the shop observing in secret the actions of the child and the shopkeeper if this was only for the
protection of the child. If evidence was to be relied on from the Officer, it may be inadmissible if no DS was in place.

Q We have reason to believe that a single person who is claiming Housing and Council tax benefit is living with an undeclared partner. We need to establish the validity of the claim by watching the house to see if the partner is in fact residing there. This will include watching the house to see if the partner's car is present and establishing whether the partner is working.

A A DS authorisation will be required for this type of activity.

Peter Purple

On 7 November 2004 you receive a complaint from the Federation of Copyright Theft (FACT) that counterfeit videos are being sold at Hot shot video rentals in Town St Wessex. 350 videos are seized which are found to be counterfeit. There are an additional 10 videos found under the counter of unclassified hard core porno-graphic videos involving children. The shop-keeper admits to the offence but is unable to provide the contact details of his supplier. He attends every Thursday to exchange video's but somehow has got wind of the investigation and has not attended since the raid despite observation of the premises on a Thursday over the last few weeks. The shop keeper only knows his supplier as being Pete who has a mobile tel number 078037 22446. There are no receipts, business card or other documents. All transactions are in cash. Attempts to make contact via this number are unsuccessful. Not long after the complaint it becomes apparent that the number is no longer in use. Enquires with other video shops in the area does not lead to any further information about the identity and whereabouts of Pete. Fill in the application form for a Data Comms.

Peter Purple

The data requested in case study reveals that a name and address which are fictitious. A further application is made to obtain details of billing arrangements. This application was made in the hope that the information may include credit card details from which a true name and address could be obtained. Unfortunately, the bill was paid in cash using a top up card. What step would you now take? Please fill in your next application form.

THE COUNCIL OF THE CITY OF BRADFORD
REGULATION OF INVESTIGATORY POWERS ACT 2000
AUTHORISATION REGISTER

APPENDIX 5

No.	Applying Officer	Department	Division	Type (Directed Surveillance(DS) / CHIS)	The subject of the Surveillance	Authorised (Yes/ No)	Authorised By	Start Date	Expiry Date	Renewed (Yes/ No)	Renewal Expiry	Date Authorisation Cancelled
					See spreadsheets for each Department marked as appendix 5 kept electronically in L\lit\rjw\RIPA2000coordination\ various The documents are set up for each department which require authorizations from time to time and are ref under the abbreviated dept name and the year the authorization was issued E.g. RIPAE&S13 The documents are accessible only to the current RIPA coordinator.							