East Cambridgeshire District Council

REGULATION OF INVESTIGATORY POWERS ACT 2000

CORPORATE POLICY & PROCEDURES

CONTENTS

FORMS

Up to date forms can be accessed at

https://www.gov.uk/government/collections/ripa-forms--2

Application forms to the Magistrates Court will be completed by Legal Services

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/approval-order-form?view=Binary

Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and crime threshold for directed surveillance – *can be accessed*

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

1.0 INTRODUCTION

1.1 This document sets out the Council's obligations under the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA came into force in October 2000 and regulates, amongst other things, types of covert surveillance that can be undertaken and the use of a person as a Covert Human Intelligence Source (CHIS).

1.2 Under RIPA the Council must have procedures in place that ensure surveillance is properly authorised, with full consideration given to the necessity and proportionality of the covert surveillance or CHIS in the context of individuals rights under the Human Rights Act 1998 (the HRA). RIPA also provides a number of safety measures in that it limits those that can or should use covert surveillance, the grounds and circumstances in which it can be used and how the material obtained must be dealt with.

1.3 The Protection of Freedoms Act 2012 has also introduced further restrictions on the ability of an Authorised Officer ('AO') to grant an application[1], and a further checking procedure of Magistrates Court approval for all applications and renewals. In the main Local Authorities have restricted powers to undertake surveillance, with more intrusive techniques restricted to intelligence and law enforcement agencies investigating the most serious crimes, including in the interests of national security. Even where this is considered an important tool to take an investigation further, this should be the exception, rather than the rule.

BACKGROUND

1.4 The HRA requires the Council and any organisations working on its behalf to respect the private life and family of citizens, their home and their correspondence. This is not an absolute right and as such the Council may interfere in the citizens' rights mentioned above, if the interference is: -

a) In accordance with the law,
b) Necessary, and
c) Proportionate.

1.5 Covert surveillance or the use of a CHIS is usually a last resort in an investigation. RIPA sets out a statutory mechanism for authorising covert surveillance or a CHIS, and this will only be undertaken where there is no reasonable and less intrusive means of obtaining the information.

1.6 Staff directly employed by the Council and external agencies working for the Council are covered by RIPA whilst they are working for the Council in a relevant investigatory capacity. The main agency that will be involved in such work for the Council is the Anglian Revenues Partnership. Authorisation of any covert surveillance or use of a CHIS, within the Council's District, will be in accordance with this Policy and authorised by the AO identified in Appendix 1.

[1] See 7A Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No 521

1.7 Compliance with RIPA/ Codes of Practice/ relevant legislation and the procedures set out in this Policy, protects the Council and its Officers against legal challenge. Section 27 of RIPA states that "*conduct…shall be lawful for all purposes if an authorisation…confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation*". Failure to abide by RIPA/ this Policy renders the Council liable to claims and/ or could affect the use of the information in any subsequent criminal proceedings. The Investigatory Powers Tribunal can also award compensation. All covert activities that are not properly authorised should be reported as soon as it is recognised to Legal Services – who will then have to report this to the Chief Surveillance Commissioner.

1.8 In addition to setting out the procedures that must be followed, this Policy aims to provide guidance to Officers about the circumstances where they are permitted to embark on covert surveillance or use a CHIS. Officers can *and should* obtain further assistance/ guidance from Legal Officers within Legal Services. Any Officer who is likely to make applications or authorise them should undertake training (which will be arranged periodically or on request by Legal Services) and in all cases Officers should be familiar with the relevant Codes of Practice, and OSC Guidance[2] before making any application, and remember that any grant by an AO, must then be followed up with an applications for approval to the Magistrate Court *before* any surveillance/ engagement of a CHIS is undertaken. 1.9 The Director (Support Services) is the Senior Officer for the RIPA process for the Council and the Principal Solicitor is the Councils RIPA Monitoring Officer. Advice can be sought from the Authoring officers or Legal Services.

1.10 Copies of the Codes of Practice can be found at the following links: https://www.gov.ukgovernment/collections/ripa-codes.

1.11 Further guidance can be obtained from the Office of Surveillance Commissioners website: https://osc.independent.gov.uk

GENERAL

1.7 There will be times when Council Officers need to conduct surveillance in the course of their investigatory duties: for example, fraudulent housing benefit claims, nuisance investigations etc. *Surveillance is a last resort that an investigator will use to prove or disprove an allegation*. Officers should always consider using other overt investigatory tools (such as community advice, warnings, signposting, inspections) before considering whether an authorisation under RIPA is required. Most of the time, however, the surveillance will be "low-level" or "overt" (see 3.1.10-3.1.11). Low-level or overt surveillance does not usually require any RIPA authorisation. However, each individual situation must be considered separately in the light of RIPA to ensure compliance.

1.8 Covert surveillance may, however, be required for some investigations; this means surveillance carried out in a manner calculated to ensure that the person subject to surveillance is unaware that it is or may be taking place and it can be **intrusive** *or* **directed**. Surveillance is *intrusive* if it is carried out by an Officer or with the use of a surveillance device, in a residential premises or private vehicle. **Local Authorities are NOT authorised to conduct intrusive surveillance.**

[2]OSC Procedures and Guidance Dec' 2014

1.9 With the exception of low-level or overt surveillance, all other surveillance carried out by the Local Authority must therefore be 'directed'. This is covert but not intrusive surveillance, conducted in a manner that "*involves the observation of a person or persons with the intention of gathering information to produce a detailed picture of a person's life, activities and associations for the purpose of a specific investigation or operation".*

1.10 There may also be situations where the use of a **CHIS** (which can be a Council employee), is required. Their use is also regulated by RIPA (under section 29). A CHIS is a person who establishes or maintains a relationship with someone in order to covertly obtain information, to provide another person with access to information or to disclose information as a consequence of that relationship. These tend to be used by the Police for undercover operations/ or for some test purchases (although for most public authorities, test purchases are unlikely to require a CHIS authorisation[3]). ***A CHIS should not be engaged/ authorised until advice has been sought from Legal Officers within Legal Services. It is extremely unlikely that Officers will be advised to authorise the use or conduct of a CHIS.***

1.11 Directed surveillance (DS) or the use of a CHIS must be carried out in accordance with RIPA and can only commence when authorisation has been granted, firstly by an Authorising Officer and then the Magistrates Court.

1.12 **Scope of this Policy**

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. Other techniques, such as some of those listed below, which are not regularly undertaken by local authorities, are not covered by this Policy.

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

- The covert use of surveillance equipment within any premises or vehicle, including business premises and vehicles, with the intention of covertly gathering information about the occupants of such premises or vehicles, unless undertaken as part of a CHIS authorisation.

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

In addition, this document does not address the detailed assessment of risks that Officers will need to undertake as part of any investigation. Normal departmental policies on identifying such risks should be adopted if it is perceived that any risk might arise from a specific operation. The CHIS authorisation form in Appendix 5 at section 8 specifically refers to risk assessment, and should be considered and completed in full before any application is considered.

[3] Home Office Covert Human Intelligence Sources Code of Practice April 2010

2.0 RELEVANT LEGISLATION

2.1 **The Data Protection Act 1998** (DPA)

2.1.1 The DPA provides eight principles to be observed to ensure that the requirements of the Act are complied with. They provide that personal data, which includes personal data obtained from covert surveillance techniques, must:

(1) be fairly and lawfully obtained and processed;
(2) be processed for specified purposes and not in any manner incompatible with those purposes;
(3) be adequate, relevant and not excessive;
(4) be accurate;
(5) not be kept for longer than is necessary;
(6) be processed in accordance with individuals' rights;
(7) be secure;
(8) not be transferred to non-European Economic Area countries without adequate protection.

Breaches of the Act can lead to prosecution and financial penalties (in the latter case, up to £500,000).

2.2 **The Human Rights Act 1998** (HRA)

2.2.1 The HRA gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights. **Article 8** of the Convention is relevant in the context of covert surveillance, in that everyone has the right to respect for his/her private and family life, home and correspondence. Private and family life must be given a wide interpretation and it may include something as simple as gaining information about a person's associates or contacts. **Article 6** of the Convention is relevant in the context of covert surveillance in that everyone has the right to a fair trial, including internal procedures or hearings, and fairness extends to the way in which evidence is obtained.

2.2.2 There should be no interference with the exercise of these rights by any public authority, including a local authority, except where such interference is in accordance with the law and is necessary. Local Authorities can only do this if the basis is to detect or prevent crime or disorder[4].

2.2.3 Non-compliance with HRA: Although it is not a criminal offence to act unlawfully, the consequences of such action is that any notices, convictions, ASBOs etc. may not be valid and the victim could take civil action against the Authority.

2.3 **The Regulation of Investigatory Powers Act 2000** (RIPA)

2.3.1 This Act and its associated regulations/ Codes tries to strike a balance between community responsibilities (including effective law enforcement), and individual rights and freedoms.

2.3.2 The use of DS or a CHIS is likely to result in obtaining private information about a person, but is permitted by RIPA and its associated regulations if such surveillance has been authorised in the manner provided by the Act, the Home Office Codes of Practice and the prescribed standard forms used.

[4] And only for "serious crime" for directed surveillance as per the Protections of Freedoms Act 2012 & SI 2012 No 2075 & see post 3.1.1

2.3.3 Home Office guidance suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement Officers as part of *general* observation does not need to be regulated by RIPA, as long as the *systematic* surveillance of an individual is not involved. Information gathered in such a way by, for example, Planning Officers, Parking Attendants, Licensing Officers and Environmental Health Officers would normally fall outside the provisions of the Act. Once surveillance becomes systematic as a means of gathering information, for example, by being carried out over a lengthy period of time or on a regular basis, it will be regarded as DS and RIPA will apply. However, it is worth noting that OSC Guidance indicates[5] that use of binoculars and cameras in relation to residential premises can be intrusive even if use is only "fleeting", if the information quality is the same as is obtained if present on the premises or in the vehicle. Care therefore needs to be taken, **as this is not lawful.**

3.0 POLICY and GUIDANCE

3.1 All Forms of Covert Surveillance

General

3.1.1 The Council will conduct its covert surveillance operations within the DPA's eight principles and restrict those operations to situations falling within the permitted exceptions of the HRA and RIPA. Additionally, the Council can only carry out surveillance for the following purpose [S.28 (3) (b) & 29(3)(b)]:-

"for the purpose of preventing or detecting crime or of preventing disorder"[6];

Previously Local Authorities were entitled to carry out covert surveillance for more extensive purposes. However, Statutory Instrument 2010/521 restricts the Council's powers, and the Council **cannot** give authorisation under RIPA for anything other than the above AND (as from 1 November 2012)[7] in respect of Directed Surveillance, can only do so if these are criminal offences that are either punishable (whether on summary conviction or indictment), by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol (or tobacco).

The Council may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval the Magistrates Court has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include dumping of waste and benefit fraud. Covert surveillance will only be used for this ground/ as this applies to criminal offences, when sufficient evidence exists and has been documented to warrant the exercise. Furthermore, surveillance must be the least harmful means of meeting that purpose and be **proportionate** to what it seeks to achieve.

3.1.2 When undertaking an investigation, it is extremely important that all reasonable alternative methods of investigation (such as overt observation, interview or changing methods of working or levels of security) are considered/ and or attempted before embarking on an application for covert surveillance.

---

[5] At Paragraph 234.

[6] And only for "serious crime" for directed surveillance as per the Protections of Freedoms Act 2012 & SI 2012 No 2075 & see following paragraphs 3.1.1

[7] See The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources)(Amendment) Order 2012 no 1500 conditions inserted into Article 7A of 2010 no 521

Procedure for Authorisation

3.1.3 All requests to conduct (other than under emergency provisions), extend or discontinue covert surveillance or use of a CHIS must be made in writing on the appropriate forms. All such requests must be submitted to one of the Council's AOs (for a list of AOs see Appendix 1). All requests must be considered and authorised in writing by an AO. An application must then be made to the Magistrates Court for prior approval and an approval order must be made before the authorisation commences and authorised activity can commence. A secure Court email address will be used and applications will be made orally to Court.

Authorisation will only be granted where covert surveillance or use of a CHIS is believed to be necessary and proportionate. The power to consider whether to grant, extend and discontinue authorisations will be limited to these Officers, in order to ensure greater independence and consistency. However, grants and renewals will then have to be subject to an approval order by the Court. Further details on this process are set out in the Home Office Guidance[8].

3.1.4 When deciding whether authorisation for DS or a CHIS is required, Officers should consider the points contained within this Policy and any Guidance given here/ Codes of Practice/ OSC Guidance/ Home Office Guidance on the Magistrates Court applications.

3.1.5 Written authorisations for a DS operation will be valid for **3 months** and for a CHIS **12 months**[9], both from the date of approval by a magistrate

3.1.6 The Council's requirements for covert surveillance should normally be carefully planned so that the necessary consultations regarding risk assessment, insurance and health and safety can be carried out and the required provisions put in place before surveillance commences. On rare occasions, covert surveillance may need to be carried out in an emergency, and authorisation will still be required (unless this is an immediate response to events- see below).

3.1.7 Surveillance that is unforeseen and undertaken as **an immediate response** to a situation this normally falls outside the definition of DS and therefore authorisation is not required. There may be occasions when officers come across events unfolding which were not pre- planned which then require them to carry out some form of observation. As the Council is no longer able to grant urgent oral authority, to conduct surveillance the officer must be prepared to explain their decisions in court should it be necessary. Therefore they should document their decisions, what took place, what evidence or information was obtained.

If later, however, a specific investigation or operation follows an unforeseen response, authorisation must be obtained in the usual way before it can commence. Under no circumstance will any covert surveillance operation be given backdated authorisation after it has commenced – as such Directed Surveillance can now only take place where this has been authorised by the Magistrates Court. Embarking upon covert surveillance or the use of a CHIS without authorisation or conducting covert surveillance outside the scope of the authorisation will not only mean that the 'protective umbrella' of RIPA is

[8] See link to Guidance on page 4 above.
[9] The exception is for juveniles – which is for one month

unavailable, and could result in the sanctions and problems detailed in 1 above.

3.1.8 **Surveillance equipment**

In the main this is a reference to CCTV, and the Council no longer maintains an ongoing CCTV system for community safety purposes (this was transferred to City of Ely Council[10]). The Council does own and maintain some fixed CCTV record only cameras in car parks. This area is now overseen by the Surveillance Camera Commissioner, who works collaboratively with the Information Commissioner (ICO). To the extent that it applies to any remaining equipment held by the Council, the Code of practice[11] indicates that under section 33 (1) of The Protection of Freedoms Act '*a relevant authority must have regard to the surveillance camera code, which sets out guiding principles that should apply to all surveillance camera systems in public places"*.

However, Covert surveillance by public authorities (as defined in Part II of the 2000 Act) is not covered by this Surveillance Camera Code. Officers must therefore consider the covert surveillance and property interference code of practice published by the Home Office for statutory guidance on the use of CCTV cameras as part of covert surveillance under the 2000 Act[12]. Should there be a requirement for CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under directed surveillance and therefore require an authorization.

Other surveillance equipment such as cameras, and audio/visual devices used for directed covert surveillance will be subject to a central register. The Internet is a surveillance device as defined by RIPA section 48(1) and use of the internet under particular circumstances might be construed as directed surveillance and require authorisation.

3.1.9 **Risks of not having correct RIPA Authorisation**

If investigators undertake covert activity to which this legislation applies without the relevant authority being obtained and the case is progressed with criminal proceedings the defence may challenge the validity of the way in which the evidence was obtained under section 78 of the Police and Criminal Evidence Act 1984. Should the evidence be disallowed by the court, the prosecution case may be lost at financial cost to the council.

The person who is the subject of surveillance may make a complaint to the ombudsman who may order the Council to pay compensation. The activity may also be challenged for breach of privacy under the Human rights Act.

A properly obtained and implemented authorization under RIPA will provide the Council with lawful authority to interfere with the rights of an individual. It is simply not enough that an authorization for surveillance is obtained. It must be properly obtained, implemented, managed, reviewed and cancelled.

[10] 20 January 2014
[11] Issued in June 2013, link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf
[12] Paragraph 1.9 of the Surveillance Camera Code of Practice June 2013.

3.1.10 GENERAL OBSERVATION & SURVEILLANCE OUTSIDE RIPA

The Home Office Code on Covert Surveillance and Property Interference indicates that certain levels of surveillance amounting to general observations in the course of law enforcement are outside the RIPA provisions. As indicated in the Home Office Guidance[13] "*Routine patrols or observation at trouble "hotspots" should not require RIPA authorisation*". However, OSC Guidance states that "*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"*[14].

The Council still must meet its obligation under the HRA and therefore surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and management of such surveillance should be the same as that of RIPA authorised surveillance, however such activity will not require approval by a magistrate.

An application should be made using the relevant RIPA application from but these forms need not make reference to the act. Authorising officers must forward copies of every NON-RIPA form to the Principal Solicitor for input onto the Central Register, within 5 working days of authorisation, review, renewal, cancellation or rejection If in any doubt as to whether or not surveillance falls within the general observation category, Officers should seek further advice from Legal officers in Legal Services.

Overt Surveillance

3.1.11 Most of the surveillance undertaken by East Cambridgeshire District Council will be overt and obvious. It requires no authorisation. There will be nothing secretive, clandestine or hidden about it; Officers such as Waste Enforcement Officers, Town Rangers, Planning Enforcement Officers and Environmental Health Officers will be going about their business quite openly.

Mechanical/electronic surveillance will also occur openly if the subject has been told that it will happen, e.g. where a noise polluter is warned, preferably in writing, that noise levels will be recorded if the problem continues, or where an entertainment licence is issued subject to conditions and the licensee is advised at the outset that officers will be visiting without notice to check that the conditions upon the licence are being met. The making of a once off test purchase also comes into this category.

Social Networks and the Internet

3.1.12 The internet is a useful investigative tool, giving access to a large amount of information which could not otherwise be obtained. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation.

3.1.13 Whilst it is the responsibility of a individual to set privacy settings to protect unsolicited access to private information and even through 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 or aren't applied. The requirement to respect the Right to Privacy of individuals is a requirement placed upon the authority, not upon the individual concerned.

[13] Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance – October 2012

[14] Note 269 OSC Procedures and Guidance Dec' 2014

3.14.5 Repeat viewing of 'open source' sites may constitute directed surveillance on a case by case basis and this should be bourne in mind.

3.1.16 Some material may be protected from view and require the subject's permission in order to view it, for example by sending them a "friend request". This is likely to constitute activity which will require CHIS authorisation.

3.1.17 Some social networking sites make users aware of who has viewed their profile, officers should not use the profiles they use in their private lives for authority research and investigation. It is not unlawful for an officer of the Council to set up a false identity for such purposes however when used for covert regular visits and monitoring purposes authorisation must be obtained. An officer of the council must not adopt the identity of a person known, or likely to be known, to the subject of interest.

3.1.18 It is essential that detailed notes be made by any officer viewing material on the internet explaining what they were seeking, why it was necessary and Proportionate to do so and why prior authorisation was not sought. Investigating Officers must forward copies of the non-RIPA authorisation form to the Principal Solicitor for input on the Social Networking Central Register, within 5 working days of authorisation, review, renewal, cancellation or rejection.

3.1.19 Where material is printed or saved consideration must be given to the Management of collateral intrusion – there may be personal data of people.

Authorisations and Central filing

3.1.20 All draft Applications for authorisation and Renewals should be sent by the AOs to Legal Services to check prior to grant. Subject to this and final consideration by the AO, if granted, a Court application will need to be made as soon as possible for an order by a Magistrate before the operation can commence. This does not, however, remove or reduce in any way the duty of the AO to determine whether the tests of necessity and proportionality have been met.

In terms of the Court application, OSC Annual Report and Procedures and Guidance require the AO attend court to explain their rationale re necessity and proportionality, although in the absence of the AO the investigator will need to attend. AOs will be responsible for ensuring that copies of all internal monthly Reviews and Cancellations are sent to Legal Services, within 5 days of completion and will be retained in the Council's Central file and each Form will have a URN. Authorising officers must forward copies of every RIPA and non RIPA forms to the Principal Solicitor for input onto the Central Register, within 5 working days of authorisation, review, renewal, cancellation or rejection.

These will then be checked / signed and date received marked on the top of the form. Relevant information will be entered onto the Central file, which is kept by Legal Services. Applicants/ AOs should also have a way of auditing the requests they receive, retaining copies and diarising relevant dates for Reviews/ Renewals or Cancellation. Investigating Officers and AOs must diarise the renewal dates – to ensure that if any authorisation needs to be renewed at Court, sufficient time is given to completing the form, complete/ make the Court application. The Home Office guidance states that out of hour's procedures for emergencies should not be used for application or renewal purposes, so failing to be organised could result in the Application not being renewed.

3.1.21 During a covert operation, recorded material or information collected will be stored and transported securely. The AO concerned will review it regularly, and access will be restricted to the Applicant Officer, the AO concerned and the Monitoring Officer (or other relevant Legal Officers from Legal Services). The AO will decide whether to allow requests for access by third parties including Council Officers. Access will generally only be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings- see 8 below for further guidance). Note that if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold for the use of Directed Surveillance, **then the authorisation should be cancelled.**

3.1.22 Once a covert operation results in an individual being under suspicion of having committed a criminal offence, he/she must be informed of this as promptly as is reasonably practicable in order to ensure his/her right to a fair trial or hearing within a reasonable time in accordance with the HRA. In a situation where it is considered that a matter gives rise to a potential criminal prosecution, any interview with the suspect must be under caution and conducted by a suitably trained Officer.

COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

3.1.23 A "Covert Human Intelligence Source" (CHIS) is defined as:
a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

- using such relationship to obtain information or to provide access to any information to another person or

- covertly disclosing information obtained by the use of such a relationship or as a result of the existence of such a relationship where the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose or (in the case of disclosure of information) it is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the disclosure in question.

3.1.24 Authorisation is for the use or conduct of a CHIS. The use involves any action on behalf of a public authority to induce, ask or assist a person to engage in conduct of a CHIS or to obtain information by means of the conduct of a CHIS. The conduct – is any that falls within the conduct in 3.1.15 or is incidental to this and covers steps taken by the CHIS on behalf of the public authority. Most will be for both[15]. This would not apply to members of the public who volunteer information / or phone contact numbers; it may apply if you have tasked them to do this – or at the very least may require a DS application, where Article 8 of the HRA (see above) is likely to be engaged. The use of a CHIS can be intrusive and high risk, requiring sufficient resources, oversight and management. The actions are about the manipulation of a relationship to obtain information and according to the Code of practice, this will engage Article 8 of the HRA and as such, if Officers wish to use someone/ or their own behaviour is likely to be use/ or they wish to engage in conduct specified in 3.1.15 above, they will need to obtain a CHIS authorisation. However, *before* authorisation is given, consideration of the special safeguards detailed in 3.1.17 - 3.1.19 are required and whether the CHIS would be managed by the Police. OSC guidance indicated that this

[15]Paras 2.4-2.8 Code on Covert Human Intelligence Sources April 2010.

may be an effective mechanism to ensure that a local authority is fulfilling its statutory responsibilities. However, if this is something that an Officer believes is likely to happen in the future, then a written protocol should be agreed to ensure that an identified CHIS is properly managed[16].

3.1.25 There are special safeguards, which apply to the use of juvenile sources under the age of 18. There are no circumstances in which a child under the age of 16 can be authorised to give information against his or her parents, or someone with parental responsibility. AOs must also abide by the Home Office Covert Human Intelligence Sources Code of Practice and S.I. 2000 No. 2793 – The Regulation of Investigatory Powers (Juveniles) Order 2000. The duration of such authorisations would only be one month and **can only be authorised by the Chief Executive or in his absence, a Director.** That stated, the juveniles can and have been used for test purchases – for sale of alcohol and age-restricted goods, and their use would not normally require a CHIS authorisation. If, however, the juvenile was required to establish a relationship/ or required to regularly go into one particular shop for this purpose then consideration must be given as to whether a CHIS authorisation is required ***before*** such activities go ahead.

3.1.26 Vulnerable individuals, such as the mentally impaired, should only be authorised as a CHIS *in the most exceptional cases* and **only by the Chief Executive or in his absence, a Director**. A vulnerable individual is a person in need of community care services because of illness, age, mental or other disability, or is unable to take care of himself, or is unable to protect himself against significant exploitation or harm.

3.1.27 Prior to authorising a CHIS, the AO shall have regard to the Code of Practice[17] and the safety /welfare of the CHIS and shall continue to have such a regard throughout. Where a CHIS is deployed, records shall be kept to comply with the Home Office Code of Practice. A "Handler" (who can be an Officer of the Council) should be designated to have the day-to-day responsibility for dealing with the CHIS and his/ her security and welfare. Further, a "Controller" should be designated to have the general oversight of the use made of the CHIS. Chapter 6 of the CHIS Code of Practice states that a Public Authority should have proper oversight and management arrangements in place for sources. **IF NONE ARE IN PLACE THEN NO AUTHORISATION SHOULD BE GRANTED.** The grant of a CHIS application would need to be approved by the Magistrates Court – who will examine the safety and security arrangements of a CHIS before approving. If the Council has no suitable arrangements then the Court will not grant these applications.

4.0 AUDIT & MONITORING

4.1 Formal monitoring and auditing of authorisations will be carried out by the Monitoring Officer/ qualified legal staff in Legal Services.

4.2 The role of the Monitoring Officer/ Legal Services will be to: -

- 4.2.1 Maintain a Central file (containing details of Authorisations).
- 4.2.2 Try to ensure uniformity of practice on issuing Authorisations.
- 4.2.3 Check each Application, Review, Renewal and Cancellation form to ensure compliance with RIPA.
- 4.2.4 Undertake quarterly audits.
- 4.2.5 Assist with applications to the Magistrates Court for approval of the grant of Directed Surveillance (and a CHIS).
- 4.2.4 Provide guidance and arrange training (where appropriate).

[16]OSC Guidance and Procedure Dec' 2014 Paras 250-252
[17]Code of Practice Covert Human Intelligence Sources April 2010

5.0 PROCEDURE FOR OBTAINING AUTHORISATION FOR DS OR USE OF A CHIS

Action to be taken by the person applying for Authorisation

5.1 Officers are advised to discuss the need to undertake DS or the use of a CHIS with their line manager before seeking an Authorisation. As indicated, options to gain the information, which is required, other than by using covert techniques should be fully explored. **Where Officers are seeking to use a CHIS, then Legal advice should be obtained *before* authorisation (see comments above on sending draft Applications and Renewals to Legal)**.

5.2 The forms for applying for a DS or CHIS Authorisation can be found at Appendices 1 & 5. The forms are available to complete on screen. Regard should be given to the guidance below when completing the relevant sections of the forms.

5.3 Following completion of Parts 1 to 12 the applying Officer should obtain a unique reference number (to enter on the top right hand side of the form), from Legal Services. The following information should also be provided to Legal Services:

- Name of Applicant.
- Applicants department.
- Type of Application (DS 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.

The completed form should then be passed to the AO (see Appendix 9).

AOs

5.4 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that, in a Local Authority setting, the AO shall be a Director, a Head of Service, Service Manager or equivalent. There is no provision for Officers of a lower rank to grant an authorisation, even in cases of urgency[18].

5.5 Authorisation by a designated AO gives lawful authority to surveillance or use of a CHIS. The Authorisation must be given in writing by the AO, except in urgent cases, when Authorisation may be given verbally, although in such instances the procedural difference and duration of verbal Authorisations, as outlined below, **should be noted**. As indicated in OSC guidance, the roles of an applicant and AO are different – "*the applicant should provide facts and evidence but it is not the role of the applicant to assert that it is necessary and proportional that is the statutory responsibility of the AO"*[19]. It is crucial for AOs to address why an authorisation is necessary and proportionate, the risk of collateral intrusion and likelihood of acquiring confidential material (see below paragraph 6).

6.0 DOCUMENTATION & GUIDANCE ON COMPLETING THE FORMS

6.1 The appropriate documentation is detailed at Appendices 1-8. Copies documentation must be held in the Central file. This file will be held for a minimum of 5 years for audit purposes.

[18] 2010/521, article 4(2).
[19] OSC Guidance and Procedure 2014 Para 71.

The DS Application form

6.2 **Introduction**

This section should include the details of the Authority/ Officer who is requesting the Authorisation and Investigation/Operation Name to which the investigation relates. The Operation Reference Number should be the RIPA central file number (URN) given to you by Legal Services as detailed above.

Section 1- specify the name and precise position of the AO e.g. *Environmental Services Manager.*

Section 2 – Set out the purpose of the operation and investigation, so that necessity and proportionality can be considered in that context.

Section 3 – A brief description of the activity to be undertaken should be given together with an outline of the purpose of the investigation – specifically what equipment will be used/ length of time this will be used/ number of officers involved.

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

Section 5 – Set out the information you hope to obtain from the surveillance. For example, this may be evidence that a person may be resident at an address when they stipulate that they are not; evidence that the target is causing a nuisance; to identify the person responsible for fly tipping; to identify the person slashing rubbish bags left out for refuse collection. You should NOT write "*to prove Mr X is guilty".*

Section 6 – The authority has only one ground for authorisation purposes i.e. for the purpose of preventing or detecting crime or of preventing disorder[20]. However, the Council **cannot** authorise Directed Surveillance for the purpose of preventing disorder *unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment or relates to the underage sale of (tobacco) or alcohol.*

Section 7 - This section is very important. YOU MUST set out the evidence of why in the particular circumstances of the case it is necessary. Consider whether all other reasonable lines of enquiry have been attempted or if not attempted, considered and discounted. Explain why it is necessary to use the covert techniques requested.

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 intrusion will be minimised. e.g. by focusing surveillance on a limited area. Applicants should give as much detail as possible in this section as AOs should pay particular regard to the information that is given. An AO must fully understand the capabilities and sensitivity levels of technical equipment intended to be used, and where and how it is to be deployed.[21] AO's should not authorise Applications that do not state whether collateral intrusion is likely, or that do not specify what steps are to be taken to minimise it, or are unclear as the technical nature of the equipment to be used/ or likely effect on collateral intrusion.

[20]Section 28(3)(b) RIPA
[21]OSC Guidance and Procedure 2014 Para 120

Section 9 – Proportionality is very important. This involves balancing the intrusiveness of the activity on the target and others who might be affected, by the need for surveillance. The activity will NOT be proportionate if it is excess in the circumstances of the case – or the information could be obtained by other means. Put simply: is this a sledgehammer to crack a nut? If YES then it is not likely to be proportionate. The AO must review this and conclude that the methods, tactic or technique proposed is not disproportionate[22]. A potential model answer should:

- address the size and scope of the operation against the perceived crime or disorder perceived;
- explain how/ why the methods will cause the least intrusion;
- explain how the means justify the end results; and
- evidence what other measures were considered and why not used[23].

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

An Authorisation, which may involve the acquisition of confidential material, may only be granted by the Chief Executive or Assistant Director (Support Services) in his absence. Where such material is acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during this next inspection and made available. Legal must be informed if such material is obtained during DS[24] and advice sought before further dissemination.

Section 11 – Self explanatory.

Section 12 – The AO must deal with the 5 "Ws" and "How" in statement form i.e. who, what, where, when and HOW. The AO must demonstrate they are satisfied with the evidence/ intelligence within the application form before authorising. They must explicitly state when they are authorising.

Section 13 - that the application is necessary and proportionate. The terms of necessity and proportionality relate to Human Rights of the target and other persons; it is essential that these matters are adequately covered in the sections above.[25]

Section 14 – Confidential information: **If authorising Confidential information** the Chief Executive/ Assistant Director (Support Services). in his absence will need to complete to show compliance with 3.1-3.12 of the Code of Practice (clink on to the link above at 1.6 for DS). If the confidential information likely to be obtained is information subject to legal privilege, then the authorisation can only be for 3 months in the first instance, and prior approval must be obtained from the OSC prior to authorisation.

The first review date should be inserted and diarised. This will generally be one calendar month from the date of Authorisation. Full name/ position of

[22]OSC Guidance and Procedure 2014 Para 73
[23]AOs should see full Para 74, OSC Guidance and Procedure 2014
[24] Paras 4.27 – 4.31 Code Covert Surveillance and Property Interference April 2010
[25] See Paras 3.3-3.7 Code Covert Surveillance and Property Interference April 2010

AO should be inserted and remember to sign, insert date and time of signature!

Sections 15 – 16 – only need to be completed if this is an urgent authorisation; therefore if not applicable, cross through the remaining part of the document.

Application for CHIS

6.4. **Introduction** – You need to set out source referral information (where relevant); "Handler", "Controller Information", and set out who will hold the source information. If a CHIS is to be sought for a third party source the Investigating Officer must have regard to the provision of section 29(5) RIPA, paragraphs 6.6-6.9 of the Code of Practice[26] and Statutory Instrument 2000 No 2725 and if appropriate 2000 No 2793 for juveniles. In particular the investigating Officer must ensure that a senior manager in his / her section is tasked with the oversight of the use of CHIS and who shall maintain the records specified in Paragraph 3 of the Statutory Instrument.

Sections 1 & 2 – see DS application above.

Sections 3 & 4 – these are reasonably self-evident; you must set out purpose of the CHIS and then how the source will be used in the operation.

Section 5 & 6– the same as DS sections above.

Section 7 - The risk of collateral intrusion in terms of risk of interference with private and family life of persons who are not the intended subjects of the CHIS activity must be considered before authorising, and measures taken to avoid unnecessary intrusion[27]. These measures / "precautions" should be set out in this section; for example: "*contact will be limited to the target; CHIS discouraged from engaging in contact that will result in third party private information being obtained, source will have contact with Handler X times per week, and source will report any infringement to Handler as soon as practical*" etc. If infringement occurs after the Authorisation, then those tasking the operation MUST inform the AO (AO) – and the AO MUST consider if the original authorisation needs to be amended or a new one issued.

Section 8 - As part of any risk assessment of the operation, you must consider whether tasking the source to act in a particular way would adversely impact on community confidence or safety. If a conflict is anticipated then seek Legal advice *before* proceeding with the operation.

Section 9 - Section 29(5) (a) and (b) of RIPA requires Public Authorities to have in place proper oversight and management arrangements for sources (see above and Code[28]). By and large the Council does not use third party sources. However, the Council must still have regard for the health and safety of Officers who act under a CHIS authorisation. The Council must carry out a risk assessment of likely risks to be faced by an Officer during the conduct of the investigation (and after the Cancellation of the Authorisation). Departmental risk assessment methods should be utilised to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered as well as the management of any requirement to disclose information tending to reveal the

[26]Code on Covert Human Intelligence Sources April 2010
[27]See Paras 3.8-3.11 of Code on Covert Human Intelligence Sources April 2010
[28] Code on Covert Human Intelligence Sources April 2010

existence or identity of a CHIS to, or in, court. Full details of the assessment should be recorded on the form.

Section 10 - Proportionality[29] is a very important consideration. This involves balancing the intrusiveness of the activity on the target and others who might be affected, by the need for the operation. The activity will NOT be proportionate if it is excess in the circumstances of the case – or the information could be obtained by other means. The source must be managed to meet this objective, and should not be used in an arbitrary or unfair way. Put simply: "Is this the least intrusive method of obtaining the evidence? If NO then it is not likely to be proportionate.

Section 11 - Confidential information includes religious material, material subject to legal privilege, confidential and personal information not connected to your investigation, and confidential journalistic information. If there is a likelihood that you may obtain confidential information the only person who can grant this is the Chief Executive. If this confidential information includes matters subject to legal privilege, then this will need prior approval from the Surveillance Commissioners.[30]

Section 12 – Self explanatory.

Section 13 - The AO must deal with the 5 "Ws" and "How" in statement form i.e. who, what, where, when and HOW.

Section 14 – see DS section 13 above.

Section 15 – see DS section 14 above.

Section 16 & **17** – you should set down the next review date, which should be one calendar month *or sooner in appropriate circumstances*. Further review dates may be arranged, but if not, they must be considered when the CHIS is reviewed.

Section 18 – time and date of signature and when Authorisations end (can be granted for up to 12 months). It can only be renewed at that time if a review has been carried out and the results considered *before* renewing.

Both forms contain a section for use in instances where verbal Authorisation has been given in urgent situations. This section of the forms should be ignored since urgent verbal authorisation can no longer be given due to the requirement to obtain judicial approval before authorised activity can commence.

The form should be considered by the AO who should complete the remaining parts of the form. In cases where approval can only be given by the Chief Executive, the application should be sent to the first level AO for initial consideration, who would then submit the form to the higher level.

Action to be taken by the AO when completing their parts of the forms

6.5 The AO must firstly consider whether the DS should be undertaken or a CHIS used. Secondly, whether the risk of interfering with a person's private and family life, whether or not the person is the target (i.e. collateral intrusion) of the surveillance, is proportionate to the objective that is to be achieved.

[29] See 3.2-3.45 of the Code on Covert Human Intelligence Sources April 2010

[30] See Parts 2 & 3 of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: matters subject to Legal Privilege) Order 2012 no 123

6.6 The question of proportionality and the risk of collateral intrusion are important considerations for the AO 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. As indicated, if there is a real risk of this then only the Chief Executive can grant. If a juvenile then only the Chief Executive or his Deputy can grant this. If this confidential information includes matters subject to legal privilege, then this will need prior approval from the Surveillance Commissioners.[31]

6.7 The AO must complete relevant sections of the Application forms and make a decision as to whether to approve or refuse the application.

6.8 Both forms require the AO to specify a date when the Authorisation should be reviewed and the frequency of review thereafter. This should normally be one calendar month after the Authorisation is granted, or sooner if there is a risk of obtaining confidential information. A Review form has to be completed (see Appendices 2 & 6) to record any review that takes place.

6.9 Draft forms must be sent to Legal services before AO/ Chief Executive approval. A copy of the completed authorisation form, whether approved or refused, should be sent to Legal Services so that a Court application can be made as soon as possible. Copes of the documents should be kept by the Investigating Officer making the application and by Legal.

7. DURATION OF AUTHORISATIONS. DETAILS ON REVIEWS, RENEWALS AND CANCELLATIONS

Authorisations

7.1 DS Authorisations will cease to have effect three months from the date of approval and CHIS authorisations, twelve months from the date approval (Juveniles under 16 are for 1 month).

7.2 It will be the responsibility of the Officer in charge of an investigation to ensure that any DS or use of a 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. Legal Services shall perform an auditing role in this respect **but the primary responsibility rests with the Investigating Officer and their relevant AO. Note also the time scales for Renewal of authorisations at Court.**

Reviews

7.4 All authorisations should be reviewed once a month whilst they are 'live'. Forms for Reviews are at Appendices 2 and 6 for Directed Surveillance and CHIS respectively. Copies should be sent to the Monitoring Officer within 5 days of completion. There is no requirement for the Magistrates Court to consider an internal review.

Renewals

7.5 The Home Office Guidance[32] states that applications for Renewals should not be made until shortly before the original authorisation period is due to expire.

[31] See Parts 2 & 3 of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: matters subject to Legal Privilege) Order 2012 no 123

[32] Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance – October 2012

This may cause practical difficulties in small enforcement teams to ensure that the Investigating Officer is available to complete a Renewal form/ have this reviewed by the AO and Legal Services before grant and then make the application to the Magistrates Court. It is therefore important when diarising renewal dates that this is factored into the management of the operation and the Renewal form competed a few weeks before so that the documents can be reviewed, granted by the AO and the application made the week that the renewal is due. 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.

7.6 The Officer requesting the Renewal should complete Parts 1 to 7 of the application to Renewal a DS or CHIS Authorisation form (to Part 9 for the latter; Appendix 3 or 7 respectively) and submit this to the AO for consideration and completion of Parts 8/10-11. The AO must consider the application for Renewal in relation to the original purpose for which Authorisation was granted, taking into account any change in circumstances. This is not a rubber stamping exercise – full consideration must be given. If the information has not been obtained during the 3 month authorisation – there must be reasons for this that may affect the necessity/ proportionality considerations for a Renewal.

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

Cancellations

7.9 It is essential that the Authorisation is cancelled when the exercise is completed and the Authorisation is not merely left to 'run its course' until the time limit expires. The responsibility to ensure that Authorisations are cancelled rests with the Investigating Officer and the relevant AO. Note again as detailed above, that if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold for the use of directed surveillance, **then the authorisation should be cancelled.**

7.10 To cancel, the person in charge of the investigation should complete parts 1 and 2 of the Cancellation of Authorisation form (Appendices 4 and 8). The form should be submitted to the AO for endorsement and completion of Parts 3 and 4. There is no requirement for the Magistrates Court to consider a Cancellation.

7.11 In all cases, as indicated, a copy of the completed forms must be sent to Legal Services. The original should be retained by the AO and a further copy sent to the Investigating Officer who has made the original application.

8. HANDLING MATERIAL OBTAINED FROM DS AND CHIS OPERATIONS

8.1 Material, or product, such as: written records (including notebook records); DVDs and tape; photographs and negatives; and electronic files, obtained under Authorisation, should be handled, stored and disseminated according to the following guidance.

8.2 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, 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 (or in any event retained for a minimum of 5 years).

8.3 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.

8.4 Material may be used in investigations other than the one that the Authorisation was issued for. However, use of such material outside the Local Authority, or the Courts, should only be considered in exceptional circumstances, and under advice from Legal Services.

8.5 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, which 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, which might prejudice any civil or criminal proceedings.
- Confidential material should be destroyed as soon possible, after its use for a specified purpose. Remember where this has been obtained inadvertently, the OSC may require sight of this when they inspect.

8.6 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 Legal Services. Note that original Application and Renewal RIPA forms will be shown to the Magistrates Court and copies taken for storage on HMCTS, in order to comply with Criminal Procedure Rules[33], and to enable the Magistrates Court to deal with queries and complaints. The Council will retain the original documents.

9.0 INTERCEPTION OF TELECOMMUNICATIONS

Part 1 of RIPA does not, however, prevent Local Authorities from lawfully intercepting its employees' e-mail or telephone communications and monitor their internet access for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems (which is covered under Part 1 the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[34].

The recording of telephone conversations connected to criminal investigations outside of the Councils monitoring at work policy for its own equipment falls under RIPA and provides, where one party to the communication consents to the interception, it maybe authorised in accordance with Section 48(4) of the 2000 Act. In such cases, the interception is treated as directed surveillance.

There may be occasions where this is required such as a witness who has text or voicemail evidence on their mobile telephone and ECDC require to examine the phone

10. COMPLAINTS ABOUT THE USE OF RIPA TECHNIQUES

[33] Rule 5
[34] SI 2000/2699

10.1 An individual may make a complaint about the use of RIPA techniques to the Investigatory Powers Tribunal ('IPT'). The IPT exists to investigate complaints about the potential conduct of public bodies, in relation to the use of RIPA on a person/ property or a person's communications data. If the Tribunal decides that there has been contravention of the legislation and the organisation concerned has not acted reasonably, they may uphold the complaint. Remedial measures such as the quashing of any warrants, destruction of any records held or financial compensation can and are imposed at the Tribunal's discretion. Complaints can be addressed to the following address: Investigatory Powers Tribunal, PO Box 33220, London, SW1H9ZQ

10.2 It is important that all staff involved in the RIPA application process take seriously their responsibilities. Careful management and adherence to this policy and procedures will assist with maintaining oversight and reduce unnecessary errors.

10.3 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

11. GLOSSARY OF TERMS

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 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 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.
Confidential Material	Includes: ▪ matters subject to legal privilege; ▪ confidential personal information; ▪ confidential constituent information; or ▪ confidential journalistic material.
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, 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.
Covert or Directed Surveillance (DS)	Means surveillance, which is, carried out in a manner calculated to ensure that the persons 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.
Immediate Response	Includes a response to circumstances or events, which, by their very nature, could not have been foreseen.
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.
Necessity	Refers to the need for surveillance (or use of CHIS). Other options of gathering the evidence etc should be considered before undertaking surveillance. Consideration as to the exact methods of covert techniques should be given/ explained.
Person	Includes any organisation and any association or combination of persons.
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).
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.
Proportionate	**Very important.** Must be considered separately from **Necessity**. Ask yourself the following question "Is there any less invasive way of finding out the information?". If the answer is no then you know that it is proportionate to carry out the surveillance. In other words proportionality is the least intrusive way to achieve the objective.
Residential Premises	Means any **premises** occupied by any person, however temporarily, for residential purposes or otherwise 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.
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. If a CCTV camera were targeted to observe a specific individual then this would fall under RIPA and would need an authorisation.
Surveillance Device	Means any apparatus designed or adapted for use in surveillance.

ECDC List of Authorised Officers- RIPA applications

Internal fraud / external fraud (ARP benefit fraud) or finance related investigations →	**AO** **LINDA GRINNELL** **FINANCE MANAGER**
Environmental and Housing Services related investigations →	**AO** **LIZ KNOX,** **ENVIRONMENTAL SERVICES MANAGER** **DAVE WHITE, WASTE SERVICES TEAM LEADER**
Planning or development related investigations →	**AO** **SUE WHEATLEY** **PLANNING MANAGER**
All investigations where the use of CCTV is requested as the primary directed surveillance in an operation →	**AO** **TRACEY HARDING** **TEAM LEADER TOWN CENTRE AND TOURSIM**

AO
CHIEF EXECUTIVE/ (IN HIS ABSENCE)
ONLY DIRECTOR (REGULATORY SERVICES) (
FOR ALL INVOLVING CONFIDENTIAL MATERIAL OR JUVENILES UNDER 16 OR VULNERABLE ADULTS

Generally Applicant Officers will apply for RIPA authorisations to the relevant AO that covers their service area. However, each of the above AO's can authorise Applications, Renewals, and undertake Reviews and Cancellations for any other ECDC service area investigation, if the Service area AO is unable to do so.