Regulation of Investigatory Powers Act 2000 (RIPA) Policy

South Oxfordshire and Vale of White Horse District Council

South Oxfordshire District Council
Listening Learning Leading

Vale of White Horse District Council

Change Record

Change Record	
Policy Title	Regulation of Investigatory Powers Act 2000 (RIPA) Policy
Version Number	V1
Owner(s)	Pat Connell
Author(s)	Pat Connell
Approved by	
Effective date	
Renewal date	

Table of Contents

Change Record 1
1 Introduction 4
1.1 Purpose 4
1.2 Scope 4
2 Use of RIPA vs Human Rights 5
3 The Investigatory Powers Commissioner's Office (IPCO) 6
3.1 Role of the IPCO 6
3.2 Requests for IPCO inspection reports 6
4 Impact of not following RIPA 7
5 Use of RIPA 8
5.2 Provisions of RIPA that apply to the councils 8
6 Types of Surveillance 9
6.2 Overt Surveillance (outside of RIPA) 9
6.3 Use of Covert Surveillance 10
6.4 Covert Human Intelligence Source (CHIS) 10
6.5 Directed surveillance. 11
6.6 Examples of types of surveillance 12
7 Private Information. 13
8 EXCLUSIONS – Where we cannot use surveillance. 14
8.2 Intrusive Surveillance. 14
8.3 Use of Children to gather information about parent/ guardian. 14
8.4 Vulnerable Individuals 14
9 Grounds for surveillance 15
10 Communications data - acquisition and disclosure of 16
11 RIPA and contracted service providers 18
12 Authorisations and roles 19
12.1 Authorisations in general 19
12.2 Applications for directed surveillance. 19

12.3 Additional factors for authorising CHIS 20

12.4 The role of Senior Responsible Officer (SRO) 20

12.5 The role of RIPA Coordinating Officer 20

13 Policy review 21

1 Introduction

1.1 Purpose

1.1.1 This policy is the framework on which the councils apply the provisions of The Regulation of Investigatory Powers Act 2000 (RIPA) as it relates to covert surveillance. It must be read in conjunction with the statutory codes of practice issued by the Secretary of State and any additional guidance provided by Investigatory Powers Commissioner's Office (IPCO). This policy is supported by a RIPA Procedure which sets out a guide to practice, responsibilities and procedure to be followed.

1.1.2 All references to the Home Office Codes of Practice relate to the latest versions which were issued in relation to covert surveillance and covert human intelligence sources, and in relation to the acquisition and disclosure of Communications Data. References to the Code of Practice and other relevant Guidance document relate to the latest version which was issued.

1.1.3 The Regulation of Investigatory Powers Act 2000 (RIPA) is the domestic law that regulates the way law enforcement agencies, and public bodies conduct surveillance for the purposes of law enforcement. The fundamental requirement of RIPA is that when the councils consider undertaking directed surveillance or using a covert human intelligence source (CHIS) it must only do so if the activity has been authorised by an officer with appropriate powers, and the relevant criteria are satisfied.

1.2 Scope

1.2.1 This policy applies to all staff and agents working for the councils. Although the councils may have limited use of the powers under RIPA, it is important that there is good awareness and knowledge across service teams so that we do not inadvertently use any approach that may contravene RIPA.

1.2.2 As the councils have a number of functions to undertake which involve the enforcement of laws and regulations, for example, environmental protection, health and safety, licensing, fraud investigation and planning enforcement, officers will need to conduct investigations and where appropriate take legal proceedings. The councils will not normally make use of covert surveillance and similar activities unless it is necessary for an investigation.

1.2.3 All investigations or enforcement actions involving covert surveillance, or the use of a CHIS must comply with the provisions of RIPA.

2 Use of RIPA vs Human Rights

2.1.1 The Human Rights Act 2000 (HRA) requires the councils to have respect for the private and family life of citizens. However, in rare cases, it may be lawful, necessary and proportionate for the councils to act covertly in ways that may interfere with an individual's rights.

2.1.2 The rights conferred by Article 8 of the HRA are qualified, so it is still possible for a public authority to infringe those rights providing it is necessary and proportionate.

2.1.3 **It is necessary:** Necessity means that in the particular circumstances of each enquiry there is no reasonably available overt method of obtaining the information that is being sought. This test will have to be applied to each case on its own merits but if there is a reasonable alternative to covert surveillance then the necessity test will probably not be satisfied.

2.1.4 **It is proportionate:** Judging proportionality will probably involve three considerations:

- Is the proposed method of surveillance excessive in relation to the seriousness of the matter that is being investigated? Is it proportional to the mischief under investigation?
- Is there a reasonable available alternative method of investigation that would be less intrusive of privacy rights? i.e. It is the only option, other overt means having been considered and discounted.
- Can collateral intrusion be avoided, and is the surveillance proportional to the degree of anticipated intrusion on the target and others? In addition to the subject there may be a possibility that the privacy rights of a third party may be infringed during surveillance.

2.1.5 By the application of authorisation procedures and Magistrates Court approval, RIPA ensures that a balance is maintained between the public interest and the human rights of individuals.

3 The Investigatory Powers Commissioner's Office (IPCO)

3.1 Role of the IPCO

3.1.1 The IPCO is overseen by the Investigatory Powers Commissioner (IPC) and supports the IPC and Judicial Commissioners in fulfilling their duties under the Investigatory Powers Act 2016. The IPCO is an Arm's Length Body of the Home Office and acts independently of the Government.

3.1.2 The IPC has responsibility for reviewing the use of investigatory powers by public authorities. This includes independent review of applications from public authorities to use the most intrusive investigatory powers and check compliance with the law.

3.1.3 The IPCO has a statutory obligation to inspect the use of investigatory powers by public authorities. Inspections will involve either an in person visit or remote access to records to scrutinise the records of any use of RIPA. As well as authorisation records and supporting documents, the review can include examining training materials and our governance structures.

3.2 Requests for IPCO inspection reports

3.2.1 The IPCO itself is not covered by the Freedom of Information Act 2000 (FOIA) and if councils receive requests for disclosure of IPCO inspection report we must respond as if the reports are our own documents.

3.2.2 Before making any disclosure, the receipt of the request should be brought to the attention of the IPCO's Data Protection Officer via info@ipco.org.uk who should be consulted with about the release.

4 Impact of not following RIPA

4.1.1 It is possible that unauthorised surveillance will be a breach of a person's right to privacy under HRA Article 8. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords.

4.1.2 If the correct procedures are not followed:

- the authorisation will not take effect as it will not be approved by the Magistrates Court if there are not reasonable grounds.
- Court proceedings that rely upon the information obtained by surveillance may be undermined.
- a complaint of maladministration may be made to the Ombudsman.
- the councils could be the subject of an adverse report by the Investigatory Powers Commissioner's Office
- a claim could be made leading to the payment of compensation by the councils.

5 Use of RIPA

5.1.1 RIPA does not;

- Make unlawful anything that is otherwise lawful.
- Impose any new statutory duties (N.B. but see paragraphs 1.5 –1.7 on the possible consequences of non-compliance)
- Prejudice or disapply any existing powers available to the councils to obtain information by any means not involving conduct that is governed by RIPA. (For example, it does not affect the councils' current powers to obtain information from the DVLA or the Land Registry).

5.1.2 If the RIPA procedures are followed correctly the conduct of an investigation will be deemed lawful for all purposes (section 27 RIPA). This protection extends to criminal and civil proceedings, and a complaint to either the Local Government Ombudsman or the Investigatory Powers Tribunal. It therefore provides protection both for the councils and any officer who may have been involved in an investigation.

5.1.3 Applications to the Magistrates' Court for approval of an authorisation must be made in accordance with the requirements of the Court.

5.1.4 The use of the powers conferred by RIPA is subject to scrutiny by the Investigatory Powers Commissioner's Office, which carries out periodic inspections of the councils' practices and procedures. Furthermore, RIPA also provides for the establishment of a Tribunal to determine complaints about the use of RIPA powers. It is therefore essential that surveillance is always carried out in compliance with RIPA, the policies and codes of practice referred to in this document and any advice or guidance that may be issued from time to time by the Head of Legal and Democratic

5.1.5 RIPA provides a means of authorising certain acts of covert surveillance for a variety of purposes. To fully understand the effects of RIPA, it is essential to understand the various types of activity that are covered, and those that are not permitted, and the purposes that will justify surveillance.

5.2 Provisions of RIPA that apply to the councils

5.2.1 The provisions of RIPA that apply to Local Authorities provide a regulatory framework that permits;

- The use of Directed Surveillance (Part 3)
- The Use of Covert Human Intelligence Sources (Part 4)
- The Acquisition and Disclosure of Communications Data (Part 5)

6 Types of Surveillance

6.1.1 Local Authorities and the Police are permitted under RIPA to carry out covert directed surveillance and to use covert human intelligence sources the definitions for each being as follows.

6.1.2 "Surveillance" includes:

- monitoring, observing, listening to persons, watching or following their movements, listening to 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, which will include cameras, video, and listening or recording devices.

6.1.3 Surveillance can be either **overt** or **covert**.

6.2 Overt Surveillance (outside of RIPA)

6.2.1 Most of the surveillance undertaken by the councils will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases officers will be going about councils' business openly (e.g., a routine inspection by an Environmental Health Officer) or will have notified the subject of the investigation that they are likely to be under surveillance. In the latter case officers need to be particularly alert to the possibility that the proposed surveillance may entail collateral intrusion into the lives and activities of persons other than the subject of the investigation (e.g., a visitor to premises). If there is the slightest possibility of collateral intrusion a RIPA authorisation should be obtained before any surveillance is carried out.

6.2.2 Surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

6.2.3 Overt surveillance does not require any authorisation under RIPA. Neither does low-level surveillance consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer.

6.2.4 Home Office guidance also 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, if the systematic surveillance of an individual is not involved. However, 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. Any such surveillance 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. It should be remembered that the councils are not permitted to undertake intrusive surveillance.

6.2.5 Use of body worn cameras should be overt. Badges should be worn by officers stating body cameras are in use and it should be announced that recording is taking place. In addition, cameras should only be switched on when recording is necessary – for example, when issuing parking tickets.

6.3 Use of Covert Surveillance

6.3.1 Covert surveillance is covert where it is 'carried out in a manner **calculated** to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place'.

6.3.2 RIPA requires the authorisation of two types of covert surveillance (directed surveillance and intrusive surveillance) plus the use of covert human intelligence sources (CHIS) or acquisition of Communications Data.

6.4 Covert Human Intelligence Source (CHIS)

6.4.1 A person is a covert human intelligence source if that person 'establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information or providing access to any information to another person, or they covertly disclose information obtained by the use of such a relationship'. Covert in this context means that it is calculated that the subject should be unaware of the purpose of the relationship.

6.4.2 A member of the public who volunteers information to the councils is not a covert human intelligence source.

6.4.3 The conduct or use of CHIS must be authorised in accordance with RIPA.

- **Conduct** of a CHIS. This is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining or passing on information.
- **Use** of a CHIS. This includes inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

6.4.4 The use of a juvenile CHIS may only be authorised for four months at a time.

6.4.5 If a CHIS authorisation includes a source that is a vulnerable person or a juvenile, then the Investigatory Powers Commissioner (IPC) must be informed within seven days of the authorisation. These types of authorisations will be kept under close review by the IPC.

6.4.6 Members of the public who report allegations of anti-social behaviour and are asked to keep a note of incidents will not normally be CHIS as they are not usually required to establish or maintain a covert relationship.

6.4.7 **Noise -** Persons who complain about excessive noise, and are asked to keep a noise diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g., the decibel level) will not normally capture private information (if non-verbal noise such as music, machinery or an alarm), and therefore does not require authorisation. Recording sound with a DAT recorder or similar, could constitute covert surveillance, although if it can be heard from the street outside, may (as per the Code of Practice) be regarded as having forfeited any claim to privacy. The easiest option is for this to be undertaken overtly – for example it will be possible to record sound if the noisemaker is warned that this will occur if the level of noise continues.

6.4.8 **Test Purchases.** Carrying out test purchases will not normally require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information, and therefore the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g., walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product e.g., illegally imported wild meat, or using covert recording equipment is likely to require authorisation as a CHIS. Similarly, using hidden recording devices to record what is going on in the shop (e.g., a hidden CCTV Camera) may require authorisation as directed surveillance. A combined authorisation can be provided if a CHIS is carrying out directed surveillance.

6.4.9 Note 251 of the OSC's 2016 Procedures & Guidance document states:
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.

6.5 Directed surveillance.

6.5.1 Directed Surveillance is surveillance that is:

- covert but not intrusive surveillance
- undertaken for the purpose of a specific investigation or operation carried out in such a manner as is likely to result in the obtaining of private information about a person (whether one specifically identified for the purposes of the investigation or operation)

- not carried out as an immediate response to events which would otherwise make seeking authorisation under RIPA unreasonable (e.g., spotting something suspicious and continuing to observe it)

6.5.2 Surveillance by way of an immediate response to events or circumstances where it would not be 'reasonably practicable' for an authorisation to be sought is not included within the provisions of RIPA.

6.6 Examples of types of surveillance

Type of surveillance	Examples
Overt	• Signposted Town Centre CCTV cameras (in normal use) • Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. • Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert, but not requiring prior authorisation	• CCTV cameras providing general traffic, crime or public safety information. • Viewing of publicly available social media profile and postings. (Use of Human Rights Act assessment needed)
Directed, **MUST be RIPA** authorised	• Covert CCTV cameras at a fly-tipping hotspot • Covert and targeted following of a benefit claimant who is suspected of failing to declare earnings from a job, can be by investigators/observation, CCTV or social media
Intrusive or interfering with private property – **WE CANNOT DO THIS!**	• Planting a listening or other electronic device (bug) or camera in a person's home or in / on their private vehicle or on their person. • Surveillance of a place used for legal consultations

7 Private Information.

7.1.1 This phrase is defined in RIPA section 26(10) as including any information relating to a person's private or family life. The European Court of Human Rights has considered this definition and has found that private life is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by HRA Article 8. The Article also protects a right to identity and personal development and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is therefore a zone of interaction of a person with others even in a public context, which may fall within the scope of "private life".

7.1.2 The fact that covert surveillance occurs in a public place or on business premises does not necessarily mean that it cannot result in the acquisition of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about them and others that they come into contact with or with whom they associate. Similarly, although the overt use of CCTV cameras does not normally require authorisation, if the camera is used for a particular purpose that involves the prolonged surveillance of a particular person, a RIPA authorisation will be required.

8 EXCLUSIONS – Where we cannot use surveillance.

8.1.1 There are some instances where surveillance is not permissible in any circumstances.

8.2 Intrusive Surveillance.

8.2.1 RIPA provides that the councils **cannot** authorise intrusive surveillance. This is covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle, whether by way of a person or device.

8.2.2 It will also be intrusive surveillance where a device placed outside consistently provides information of the same or equivalent quality and detail, as might be expected if it were in the premises or vehicle.

8.2.3 Residential premises are any part of premises occupied for residential purposes or living accommodation, including hotel rooms or prison cells. However, it does not include common areas in blocks of flats and similar premises.

8.2.4 Private vehicle is a vehicle used primarily for private purposes by the owner or person entitled to use it.

8.2.5 Only the police or other law enforcement agencies are permitted to employ intrusive surveillance. Likewise, the councils have no statutory powers to interfere with private property.

8.3 Use of Children to gather information about parent/ guardian.

8.3.1 Authorisation may not be granted for the conduct or use of a source under the age of sixteen where it is intended that the purpose is to obtain information about their parent or any person who has parental responsibility for them.

8.3.2 Should there be an exceptional case where children are to be used as a CHIS, and this is not for the use described above, authorisation must at a specified level and for Local Authorities this is the Head of Paid Service.

8.4 Vulnerable Individuals

8.4.1 A vulnerable individual is a person who is, or may be, in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an individual may be vulnerable, they will only be authorised as a CHIS in the most exceptional of circumstances.

8.4.2 The use of a vulnerable individual as a CHIS requires authorisation at a specified level and for Local Authorities this is the Head of Paid Service.

9 Grounds for surveillance

9.1.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a custodial sentence of a maximum term of at least 6 months' imprisonment, or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

9.1.2 Even if the person granting the authorisation believes that the authorisation is necessary, they must also be satisfied that the authorised activity is proportionate to what is sought to be achieved by it. This requires the Authorising Officer to balance the need for surveillance with the level of intrusion into any person's privacy.

9.1.3 Consideration should be given to collateral intrusion, which is interference with the privacy of persons other than the subject(s) of the surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

9.1.4 Confidential information. Careful consideration is also needed when there is a risk of obtaining confidential information. The Covert Surveillance and Property Interference defines this as:

"information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above 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 any legal obligation of confidentiality. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records".

9.1.5 In cases where it is likely that confidential information will be acquired the authorisation must be granted by the by the Head of the Paid4 Service (or in their absence by an authorised Head of Service).

9.1.6 An application for an authorisation must include a full assessment of the risk of any collateral intrusion or interference so that the Authorising Officer can consider this.

9.1.7 Authorising Officers must always consider the need for surveillance or CHIS and balance this against an individual's right to privacy under the Human Rights Act 1998. An officer seeking an authorisation should always be able to justify why it is necessary and why other, less intrusive, forms of investigation are unsuitable or have previously been tried without success and thus the matter has escalated to the requirement for covert surveillance.

10 Communications data - acquisition and disclosure of

10.1.1 The Investigatory Powers Act 2016 ('IPA') provided an updated framework for lawful acquisition of Communications Data, include the who, where, what, when and how a Local Authority can obtain communications and Communications Data.

10.1.2 The IPA sets out the three powers, under sections 60A, 61 and 61A, which can be used to authorise the acquisition of Communications Data (CD), dependent on the statutory purpose and urgency. Only section 60A is relevant to local authorities, although a number of new offences would also apply in terms of unlawful acquisition and disclosure of Communications Data.

10.1.3 Public Authorities can only apply if this is for 'the applicable crime purpose'. This means the data has to be wholly or partly Events data, the purpose of preventing or detecting serious crime; or in any other case, the purpose of preventing or detecting crime or of preventing disorder.

10.1.4 The types of Communications Data that Local Authorities' can access are Entity and Events Data, which are defined as:

- **Entity Data**: means any data which is about —
  (a) (i) an entity, (ii) an association between a telecommunications service and an entity, or (iii) an association between any part of a telecommunication system and an entity,

  (b) consists of or includes data which identifies or describes the entity (whether or not by reference to the entity's location) and is not events data.

- **Events Data:** any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time. Where the purpose of the acquisition is to prevent or detect crime, and the data required is events data, the offence or conduct of the offence being investigated must meet at least one of the definitions of serious crime.

10.1.5 The IPA has also removed the necessity for local authorities to seek Magistrates or Justice of the Peace approval to acquire Communications Data. All such applications must now be processed through the National Anti- Fraud Network (NAFN), who will consider the application prior to submitting this for approval to the Office for Communications Data Authorisations ('OCDA').

10.1.6 All applications must be approved before Communications Data is acquired. The Investigatory Powers Commissioner oversees the use of the powers (who with Judicial Commissioners have a role to approve authorisations to identify or confirm the identity of a journalist's source). The application process has otherwise been made more efficient through the ability to submit these electronically.

10.1.7 Sections 37 to 44 of the Police, Crime, Sentencing & Courts Act 2022 (PCSCA) came into force on 8 November 2022. This provides public authorities with a further power to extract data held on electronic devices.

10.1.8 Before action is taken, there must be a reasonable belief that information stored on the device will be relevant for one of three scenarios and satisfaction that the extraction of the information is necessary and proportionate to achieve the purpose.

10.1.9 The three scenarios provided under s37(2) are for the purpose of:

a) preventing, detecting, investigating or prosecuting crime;

b) helping to locate a missing person; or

c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.

10.1.10 To ensure any extraction of stored communication under s.37 remains lawful, it is essential that the criteria and procedures set out within the PCSCA and the association Code of Practice are fulfilled.

10.1.11 A failure to follow these procedures correctly could result in a s.3 IPA offence (unlawful interception) being committed.

11 RIPA and contracted service providers

11.1.1 It is important to note that the legislation does not only affect directly employed council staff. Where external agencies are working for the councils, carrying out the councils' statutory functions, the councils remain liable for compliance with its duties. It is essential that all external agencies comply with the regulations, as they are contractually obliged to do so. Therefore, work carried out by agencies on the councils' behalf should be properly authorised by one of the councils' designated Authorising Officers and requires Magistrates Court approval for applications and renewals. Authorisation for surveillance should not be sought on behalf of another statutory or other organisation or agency. The advice of the Senior Responsible Officer ('SRO') should be sought in the event of uncertainty.

12 Authorisations and roles

12.1 Authorisations in general

12.1.1 Authorisations may only be given by the Authorising Officers listed in the councils' RIPA procedures. Only the Head of Paid Service can authorise the use of a CHIS for a vulnerable person or juvenile or the acquisition of confidential information.

12.1.2 Applications for the acquisition of Communications Data can only be issued by a Home Office accredited single point of contact (SPoC). The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities.

12.1.3 Local authorities using the NAFN SPoC service will still be responsible for scrutinising the application for Communications Data prior to contacting NAFN.

12.1.4 The applicant officer must complete application forms in their entirety.

12.1.5 Authorisation under RIPA is quite separate from delegated authority to act under the councils' Scheme of Delegation. **RIPA authorisations are for specific investigations only and must be cancelled or renewed once the specific surveillance is complete, or about to expire.**

12.1.6 The Authorising Officer should not just "sign off" an authorisation, they must give **personal consideration** to the necessity and proportionality of the proposed action prior to applying to the Magistrates Court for approval and must personally ensure that the surveillance is reviewed and cancelled.

12.1.7 Any rejected applications must be entered into the RIPA log held by the RIPA Coordinating Officer.

12.2 Applications for directed surveillance.

12.2.1 In the case of applications for authority to carry out **directed surveillance** the Authorising Officer should:

- consider the relevant Codes of Practice
- consider whether the specific operation or investigation has been adequately described.
- be satisfied as to the reasons for the application.
- be satisfied that the directed surveillance is **necessary** in the circumstances of the particular case.
- be satisfied that the surveillance is **proportionate** to the stated purpose and objectives.
- be satisfied that the possibility of collateral intrusion has been avoided or minimised.
- consider the likelihood of confidential information being acquired.
- check that an appropriate review period has been listed on the application form.

12.2.2 **If there is an alternative practicable means of carrying out the surveillance, which is less intrusive, then the surveillance is neither necessary nor proportionate and should not be authorised. The least intrusive method should be used.**

12.3 Additional factors for authorising CHIS

12.3.1 In addition to considerations 12.2 above, when authorising the conduct or use of a CHIS the Authorising Officer must:

- be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved.
- be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS.
- consider the likely degree of intrusion of all those potentially affected.
- consider any adverse impact on community confidence that may result from the use or conduct, or the information obtained.
- ensure **records** contain statutory particulars and are not available except on a need-to-know basis.
- ensure that authorisations relating to the use of a juvenile CHIS are only for four months at a time.
- be satisfied that a full risk assessment has been undertaken.

12.4 The role of Senior Responsible Officer (SRO)

12.4.1 The councils' SRO is the Head of Legal and Democratic. The SRO is responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance
- compliance with Part 2 of the Act and with the Codes
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
- engagement with the IPCO inspectors when they conduct their inspections, where applicable
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

12.5 The role of RIPA Coordinating Officer

12.5.1 The councils' RIPA Coordinating Officer is the Deputy Head of Legal (Operational) who is responsible for:

- dealing with the CHIS on behalf of the councils
  - directing the day-to-day activities of the CHIS
  - recording the information supplied by the CHIS
  - monitoring the CHIS's security and welfare.

13 Policy review

13.1.1 This policy will be kept under review and updates on at least an annual basis and will be presented to the Joint Audit and Governance Committee annually for approval.