

Canterbury City Council

Surveillance Policy

Regulation of Investigatory Powers Act 2000

Mark Ellender
Head of Legal and Democratic Services
Canterbury City Council
Military Road
CANTERBURY
CT1 1YW

2010 version



CANTERBURY CITY COUNCIL

POLICY DOCUMENT

GUIDE TO OFFICERS

REGULATION OF INVESTIGATORY POWERS 2000

1. Introduction
2. Relevant Legislation
3. Implementation
4. Policy

Appendix 1 List of Authorising Officers

Appendix 2 Flowchart (Procedure)

Appendix 3 Explanatory Notes

Appendix 4 Interception of Communications

Mark Ellender
Head of Legal and Committee Services
Canterbury City Council
Military Road
CANTERBURY

1. Introduction

- 1.1 The Regulation of Investigatory Powers Act 2000 has impacts on local authorities in the various areas of enforcement but also has relevance to employee matters, for example, the interception and monitoring of e-mails. A failure to comply could prove fatal to a successful prosecution. All steps must be taken to ensure compliance with the requirements of the Act.
- 1.2 Several of the Councils' activities will involve Covert Surveillance of individuals and organisations. Examples include Benefit Fraud, Licensing, Planning Enforcement and Noise Complaints.
- 1.3 Following the introduction of the Human Rights Act 1998 (HRA) such surveillance could be a breach of that Act. However, the HRA allows surveillance where it is lawful. Consequently The Regulation of Investigatory Powers Act 2000 (RIPA) has been introduced to make lawful certain types of surveillance. It also sets out a statutory framework for the granting of authority to carry out surveillance. RIPA came into force in October 2000. It includes local authorities within those bodies (namely public bodies) which it controls.
- 1.4 Covert surveillance is surveillance that 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 surveillance is increasingly becoming the subject of legislative controls. The requirements of the Data Protection Act 1998 (DPA) and the HRA that have to be borne in mind in overt surveillance need to be considered also in the area of covert surveillance. RIPA is also of relevance whenever covert surveillance of an identifiable or named person is carried out by a public authority carrying out an investigatory function. The use of covert human intelligence sources (CHIS) is also regulated by RIPA. A CHIS is a person who established 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.
- 1.5 Covert surveillance can be either:
 - 1.5.1 Intrusive Surveillance means surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle by an individual on the premises or in the vehicle or is carried out by means of a surveillance device. A

surveillance device not on or in the premises/vehicle will only be intrusive if it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually on/in the premises/vehicle.

- 1.5.2 Directed Surveillance means Covert but not Intrusive surveillance undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather information about them. There is a process to be followed to enable such activities to be authorised which is outlined in the flowchart and the notes to it at Appendix 2 and Appendix 3. The text of this document deals with the issues in more detail.
- 1.6 All interception of Communications must be carried out in accordance with the provisions of the Regulation of Investigatory Powers Act 2000 and the Codes of Practice which accompany the Act and whose provisions must be observed. Local authorities can carry out interception of communications in a restricted number of circumstances. They can only carry out interception where an interception warrant is not required as the Council is not an agency that can apply for such a warrant.
- 1.7 The Council's approach to the use of these powers is a cautious one and contained in appendix 4 to this policy. Before any use of these powers is contemplated advice should be sought from the Head of Legal and Democratic Services or in his absence the Deputy Head of Legal Services.

2. Relevant legislation

The Data Protection Act 1998

- 2.1 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 compatible 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.

The Human Rights Act 2000

- 2.2 The HRA gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights. Article 8.1. 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.
- 2.3 These are however qualified rights, in that a public authority may infringe them in accordance with Article 8.2. The conditions are that the infringement should be in accordance with the law (this being the urgent reason for RIPA). There was no remedy in law in the United Kingdom for the invasion of privacy until the Human Rights Act and then RIPA set it all out. Then following Article 8.2, RIPA says that infringements may be made if they are authorised as being necessary and proportionate and the Covert Surveillance takes place in accordance with the authorisation. If all this can be demonstrated to be in order, the infringement of privacy is “lawful for all purposes” (s.27(1) of RIPA). Consequently the Council can use evidence obtained by means of covert surveillance in criminal prosecutions or in tribunals, such as an employment tribunal if a member of staff is dismissed for some serious misconduct. In reverse, the Council and any individual officer can rely on the lawfulness of what has been done if an action is brought for invasion of privacy under s.7 of the Human Rights Act, s.13 of the Data Protection Act or by way of complaint to the Local Ombudsman or the Investigatory Powers Tribunal, who can adjudicate on complaints against a local authority. All of these recourses can engender damages, costs and unwelcome publicity; but if the activity by the authority was lawful for all purposes there should be a complete defence.
- 2.4 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.
- 2.5 Consequently, there is to 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 in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or

crime, for the protection of health and morals, or the protection of the rights and freedoms of others. **The Regulation of Investigatory Powers Act 2000**

- 2.6 This Act and its associated regulations also follow the philosophy of recent legislation in trying to strike a balance between community responsibilities, including effective law enforcement, and individual rights and freedoms.
- 2.7 Directed Covert Surveillance, including a situation where a CHIS is used, that is likely to result in obtaining private information about a person 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. Authorisation for Directed Surveillance can be granted by the Authorising Officer of a public authority if it is for certain specified purposes. Formerly authorisation could be granted for the purpose of protecting public health, but now there is only one purpose for which a local authority can use RIPA.
- 2.8 The only reason for a local authority to use any form of Covert Surveillance is “the preventing or detecting crime or preventing of disorder”. There will be strict limits on the activities which a local authority’s authorising officers can entertain an application; within these limits officers should be allowed to grant sensible applications, since the statutory instrument is not intended to frustrate activities falling within local authorities’ statutory duties. All the same, there will be, as there have always been some activities which cannot be authorised. In such circumstances, s.80(c) provides that RIPA shall not be construed so as to prejudice any power to obtain information by means which cannot be authorised: in other words the statutory duty should still be fulfilled. There may be occasions when, the law on many issues under RIPA having received no judicial interpretation, it may be wise to play safe and obtain an authorisation; but it is plain that many investigations, at least in their early stages, do not involve any offence and fall outside the scope of RIPA and SI 2003/3171.
- 2.9 Home Office guidance suggests that the use of equipment such as binoculars or cameras to reinforce normal sensory perception used as part of general observation carried out by public authority officers engaged in law enforcement will not 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 will consequently 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 Directed Surveillance and RIPA will apply.

3. Implementation

3.1 The first version of this Policy was developed in consultation with representatives from Legal Services, Planning Enforcement, Environment and Street Scene, acknowledgement is also given to Dave Randall of Dover District Council for his assistance in preparing it. It has subsequently been revised. From 2010 it will be subject to annual member approval.

3.2 This Policy is operational and as amended from time to time will apply to all Council staff and contractors employed by the Council. All relevant Council contracts will include a term that this Policy and the Council's associated procedures are to be observed by any contractor operating on behalf of the Council.

3.3 A copy of this Policy Document will be made available for Public Inspection at the Council offices.

3.4 Codes of Practice have been issued under RIPA and are revised periodically. All are available under the publications section of the Home Office website (<http://security.homeoffice.gov.uk/ripa/>). They are of great importance and regard must be had to them when conducting any relevant Surveillance operation. A current set of forms is also available on line but these should be obtained from Lyn Wood in Legal and Democratic Services so that a check can be kept on operations. If time does not allow, a set may be downloaded.

3.5 Interception of Communications Code of Practice

The following are the current Codes of Practice:-

- Interception of Communications Code of Practice
Guidance on the procedures that must be followed before interception of communications can take place under those provisions.
- Acquisition and disclosure of communications data code of practice
Guidance on the procedures to be followed when acquisition of communications data takes place.

- Covert Surveillance Code of Practice
This code relates to authorisation of covert surveillance.
- Covert Human Intelligence code of practice
This code applies to every authorisation of the use or conduct by public authorities of covert human intelligence sources.
- Code of Practice for the investigation of protected electronic information (887K)
This code of practice explains laws relating to investigating protected electronic information.

Policy

4. All Forms of Covert Surveillance

- 4.1 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. Covert surveillance will only be carried out by the council for permitted purposes which are currently restricted to the purpose of preventing or detecting crime or prevention of disorder.
- 4.2 Surveillance equipment will be installed, or a CHIS used, by the Council for the only legitimate purpose of preventing or detecting crime or of preventing disorder – for which it is currently authorised. It may only be used when sufficient evidence exists and has been documented to warrant the exercise and surveillance is shown to be both the least harmful means of meeting that purpose and proportionate to what it seeks to achieve. It is extremely important that all reasonable alternative methods to resolve a situation, such as naked-eye observation, interview or changing methods of working or levels of security, must be attempted first and recorded in writing and the reason for surveillance being requested fully documented. This is vital to demonstrate both the necessity and the proportionality of the surveillance and alternative methods of obtaining the information must be borne in mind when considering both necessity and proportionality. Where the subject of covert surveillance is an employee, the Council's Monitoring Officer must be informed.
- 4.3 All requests to conduct, extend or discontinue a covert surveillance exercise or use of a CHIS must be made in writing on the appropriate forms. All such requests must be

submitted to an Authorising Officer of the Council. These officers are named in Appendix 1. All requests must be considered and authorised in writing by an Authorising Officer, before any covert surveillance operation can commence. Authorisation will only be granted where covert surveillance or use of a CHIS is believed by the Authorising Officer to be necessary and proportionate. The power to grant, extend and discontinue authorisations will be limited to these Officers only in order to ensure greater independence and consistency. Written authorisations for a Direct covert surveillance operation will be valid for a maximum of 3 months and for a CHIS a maximum of 12 months, both from the date of the original authorisation or extension.

4.4 If the authorisation is given by an individual directly involved in the investigation this fact should be recorded. An instruction to create surveillance should record not only the date but the time.

5. The Council's requirements for how an authorising officer should approach his or her task

5.1 The Authorising Officer must believe the activities authorised are necessary on the statutory grounds ie in the case of the council, for the purposes of preventing or detecting crime or of preventing disorder. If that is the case the Authorising Officer must also believe that they are proportionate to what is sought to be achieved by carrying them out.

5.2 Therefore authorising officers must have satisfied themselves that the invasion of privacy was both necessary and proportionate. The main evidence for this will be the authorisation itself. The authorising officer, who is the key to the whole issue of protection under s.27(1), must be able to show that he has applied his mind to these two critical issues. He should make clear by his remarks that he has done so and carry those on separate sheets of paper if the relevant box on the form is not sufficient.

5.3 What, then, is the meaning of necessity and proportionality? Necessity is not difficult: the issue is the use of covert means to discover information and covert means cannot be "necessary" if there are reasonably available overt means of finding the same information. However, since every investigation under RIPA affects one or more

particular individual each of whom enjoys privacy rights, there must also be adjudged to be necessity in that particular case, - hence the box for this purpose in the Home Office set of recommended forms – for the reason just described, and it is not enough merely to say that it is necessary for the preventing or detection of crime or the prevention of disorder. There is helpful guidance to be found on proportionality in the Revised Home Office Code of Guidance and Authorising Officers should have regard to it. “Proportionality” is more complex: the method to be used to collect the information should not be “over the top” by relation to the seriousness of the offence or disorder which is the objective of the surveillance. Next, the method of investigation chosen should be the least invasive of the target person’s privacy. It must be emphasised that only if the exact method of surveillance is in accordance with the authorisation does the immunity in S.22 prevail. Lastly, if there is to be collateral intrusion on members of the public they too have Article 8.1 rights and the impact upon their privacy must, at least, be minimised. It will not matter unless their privacy is infringed by placing photographs or other descriptive material into the public domain but this can only be achieved, because the material is disclosable in both criminal proceedings, by arranging for it to be edited out of court papers. It should not be destroyed, as this carries a serious risk that the evidence will be challenged as to its “continuity”.

- 5.4 The Council’s requirements for covert surveillance will 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. In the event of covert surveillance needing to be carried out in an emergency, authorisation is still required. In an extreme situation where it is not possible for the Requesting Officer to complete the form, the Authorising Officer must still be consulted. The revised Home Office Code of Practice on Covert Surveillance and Property Interference makes provision for oral authorisation to be granted. In such cases a record that the authority officer has expressly authorised the action should be recorded in writing by both the authorising officer and the applicant as soon as is reasonably practicable, together with the information set out in the Code. An authorisation will not be given where the need for it has been neglected or the urgency is of the authorising officer’s or the applicant’s own making.. Surveillance that is unforeseen and undertaken as an immediate response to a situation when it is not reasonably practicable to obtain authorisation falls outside the definition of Directed Surveillance and therefore authorisation is not required. If later, however, a specific investigation or operation is to follow an unforeseen response, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert

surveillance operation be given backdated authorisation after it has commenced. It is likely to be very rare for an urgent authorisation to be sought. It is also to be noted that a local authority is very unlikely to seek the use of covert surveillance in order to discover confidential material of any sort; if this is the object, legal advice should be sought. 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 unavailable but may result in disciplinary action being taken against the Officer/Officers involved.

- 5.5 Surveillance equipment will only be installed with the necessary authorisation of the Council's Authorising Officers. It will only be installed in residential premises if a member of the public has requested help or referred a complaint to the Council and such matter can only be investigated with the aid of covert surveillance techniques after all the issues referred to have been considered. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant.
- 5.6 Any request by a Council Officer to a resident to keep a video/written diary as part of an evidence-gathering exercise is not likely to be regarded as a covert surveillance exercise conducted on behalf of the Council but guidance should be sought from the monitoring officer if there are any unusual features of the case.
- 5.7 If an officer wishes to seek an authorisation for covert surveillance or use of CHIS an authorisation document should be obtained from Lyn Wood in the Legal and Democratic Services department. She will enter the relevant reference number showing the year and the number of the form in that year and send it to the officer. The forms will be numbered sequentially in each year. The authorising officer is responsible for the return of the original completed form to the Council's Monitoring Officer and is advised to keep a copy for his own purposes.
- 5.8 Authorisations normally last for three months but they are to be proportionate to the task and have as short a life as possible to achieve only what is necessary. They should be reviewed regularly. After they have fulfilled their purpose, they must be cancelled and the Monitoring Officer notified with the completed cancellation form.
- 5.9 If the Investigating Officer believes further surveillance is necessary then before the expiry of the authorisation he must ask the authorising officer to review it and make a case for renewal. A renewal requires the authorising officer to consider cancelling the

authorisation if it has achieved its purpose or will obviously fail to do so; or whether it should be replaced by an authorisation of a more promising nature. Ultimately cancellation is required in every case.

- 5.10 In accordance with the Home Office Code of Conduct certain levels of surveillance amounting to general observations in the course of law enforcement can be regarded as “low level” surveillance area and are consequently outside the RIPA Provisions. An example of low level surveillance is where a Planning Enforcement Officer merely drives past a site to check whether or not planning restrictions are being adhered to. However, should officers revisit the site this would be regarded as systematic and RIPA authority will be required. If in any doubt as to whether or not surveillance falls within the “low level” category, officers should seek further advice.
- 5.11 Overt surveillance does not require any RIPA authorisation. Consequently if verbal notification or a letter is sent to the subject of the surveillance notifying them of the kind of surveillance that is proposed, then RIPA authorisation is not required. In the case of a letter however, it is important to ensure that the letter is actually communicated to the subject and Registered Post or hand delivery should be used unless it can be established that the recipient actually received the letter. All such letters and verbal communications should only last for a maximum of three months.
- 5.12 No covert operation will be embarked upon by a Council Officer without detailed consideration of the insurance and health and safety implications involved and the necessary precautions and insurance being put in place.
- 5.13 During a covert operation, recorded material or information collected will be stored and transported securely. It will be reviewed daily and access to it will be restricted to the Senior Responsible officer, Authorising Officers and the Authorised Officer concerned. The Senior Responsible Officer 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).
- 5.14 Any video tape and audio tapes used will be identified uniquely and erased prior to re-use. A register will be kept of all tapes used to control the period of time they are retained (31 days) if not required for evidential purposes and the number of times they are re-used before being destroyed.

5.15 Once a covert operation results in an individual being under suspicion of having committed a criminal or disciplinary 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 or, if appropriate, the police must be involved immediately to ensure that evidential procedures and the requirements of current legislation are observed. The register referred to will include a note of any recorded material handed over to the police.

5.16 The Council's Monitoring Officer will act as The Head of Legal and Democratic Services in his capacity as the Senior Responsible Officer, who is to be responsible for

- the integrity of the process in place within the council for the management of Directed Surveillance and CHIS
- compliance with Part 2 of the Act and with the Codes made under it
- engagement with office of Surveillance Commissioners when they conduct their inspections, and
- where necessary, oversight of the implementation of post inspection action plans approved by the relevant Oversight Commissioner.

In consultation with the officers concerned he may cancel an authorisation if it no longer appears justified.

5.17 A register will be maintained by the Authorising Officers of all reviews of material recorded and collected covertly. They will ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice.

5.18 Before becoming an Authorising Officer such an officer must attend training for the purpose. They will be a Director, a Head of Service, a Service Manager or the equivalent.

6. Use of a CHIS

6.1 The use of vulnerable individuals, such as the mentally impaired, for a CHIS purpose should only be authorised in the most exceptional cases. Authorising Officers should also abide by the Home Office Code of Conduct relating to Juveniles.

6.2 Where the use of a CHIS is deployed, 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 the security and welfare of the CHIS. Further, a “Controller” should be designated to have the general oversight of the use made of the CHIS.

Prior to the authorising of a CHIS, the Authorising Officer shall have regard to the safety and welfare of the CHIS and shall continue to have such a regard throughout the use of the CHIS.

That were a CHIS deployed, records shall be kept to comply with the Home Office Code of Practice.

Any failure to comply with the procedures in place for the implementation of the covert surveillance policy may be a disciplinary offence.

6.3 “CHIS” is the statutory term for a police informer, and much of RIPA Part II is concerned with activities carried out by the law-enforcement agencies. However, a CHIS can also play a part in a local authority’s enforcement or internal audit procedures. If a member of the public is asked to keep a diary of noise interruptions from next door, or provide a little information additional to that already given by letter, telephone etc, that person is not necessarily turned into a CHIS: there has to be a “personal or other relationship”, the meaning of which expression has not yet been clarified by the Courts. The tests for the authorisation are the same as for directed surveillance – necessity and proportionality – to which must be added the requirements of s.29(5) and the Source Records Regulations (SI 2000/2725). There may be mandatory items in these Regulations which ‘must’ be recorded. If they are irrelevant then the Authority Officer may say so, but it should be clear on the face of the form that he or she has shown an awareness of the Regulations and sought to record what is pertinent. Reasons should be given for acting in the way shown on the form. There will always be the need for a risk assessment. As for the rest of these requirements, the authorising officer should indicate in the form that he has taken them into due account.

LIST OF AUTHORISING OFFICERS:

Environment Department

e

Roger Vick, Commercial Health Manager

Christopher Wallis, Street Scene Manager

Corporate Services Department

Andrew Stevens, Head of Revenues

Mark Gilmore, Benefits Manager

Mark Redhead, Audit and Exchequer Manager

Chief Executive's Department

Mark Ellender, Head of Legal and Democratic Services (Monitoring Officer and Senior Responsible officer)

Community Department

Larissa Laing, Head of

EXPLANATORY NOTES

The notes which follow are numbered to match the diamond shaped lozenges attached to certain boxes in the Flowchart at Appendix 1.

Note 1 Before submitting the application for Authorisation, the officer whom it is intended will conduct the surveillance must satisfy himself/herself that the following criteria have been met:

- (a) The surveillance will be covert (see paragraph 1.4 of main text).
- (b) There are proper grounds for surveillance (see the council's policy) 'The Council's requirements – how an authorising officer should approach his or her task'.
- (c) The degree of surveillance will be proportionate to what it is desired to achieve (see the council's policy) 'The Council's requirements – how an authorising officer should approach his or her task'.

Note 2 For an Application, the form should be completed by the officer due to conduct the surveillance in detail, so that the authorising officer has sufficient information to form a judgement in accordance with the Council's policy.

Notes 3, 4 and 5 Although not required for the completion of the Application Form, it may assist officers to determine which type of surveillance is being contemplated, as this may be an issue in any Court proceedings which may result. However, please note that Intrusive Surveillance as described in the introduction to this policy is not available to the Council.

Note 6 Under normal circumstances, the Authorisation must have been approved by the entitled officer (usually a Principal Officer or above) before the specified surveillance can take place.

Where time is short and an entitled officer cannot be found or cannot be contacted on the telephone, Team Leaders may authorise surveillance. In such cases, proper Authorisation should be obtained at the first practical opportunity.

In some urgent cases, surveillance may be conducted without written Authorisation (see paragraph 5.4 of main text).

Note 7 Surveillance may **only** be conducted by the officer named in the Authorisation and **only** as described in the form and in strict accordance with any conditions applied to the surveillance.

Note 8 Authorising Officers should note that surveillance will be authorised for three months, but it should be reviewed regularly as may be appropriate to the task involved.

Note 9 Where an extension to time (renewal) of Authorisation is required, application should be made in sufficient time to ensure that it can be authorised by the entitled officer.

Interception of communications

NOTE: These provisions can only be used after having taken advice from the Head of Legal and Democratic Services or the Deputy Head of Legal Services and in no other circumstances.

1. A RIPA interception warrant not required: -

(a) In the course of normal business practice.

The Council is allowed to intercept communications if it is done as part of normal business practice, for example:-

- The opening of post for distribution throughout the Council
- The logging of telephone calls, for the purpose of cost allocation, identification of private calls for reimbursement, comparative benchmarking, identification of efficiency savings, and identification of misuse of the system.
- The logging of e-mails sent / internet access for the purpose of private reimbursement.

Logging of calls etc may also fall outside R.I.P.A. if it only records traffic data, as this is not classified as interception of communications.

(b) Consent of both parties.

Both the sender **and** the intended recipient of the communication have given consent to the interception.

This also applies where the person doing the interception had reasonable grounds for believing both parties had consented to it.

(c) Consent of one party.

Either the sender **or** the intended recipient has given consent to the interception. This comes within directed surveillance and hence authorisation for directed surveillance should be sought.

2. A RIPA warrant is required:

Without consent.

An interception warrant **must** be obtained and hence the Council cannot carry out this activity on its own behalf.

However, there are various agencies that can apply for a warrant, and section 11 of R.I.P.A. gives those agencies the power to require others to provide assistance.

The person upon whom such a warrant is served has the duty to take all reasonably practicable steps to carry out the requirements of that warrant.

3. Procedure for in house interception.

- (a) As part of normal business practice.

The controller of a telecommunications system must make all reasonable efforts to inform potential users that interceptions may be made.

This will be done by means of the formation of an acceptable use policy whose terms will be notified to all staff.

All staff will be informed that certain interceptions will be carried out as part of the normal operation of the Council.

- Monitoring internet access
- Monitoring e-mail usage
- Telephone call logging
- Opening post for distribution

- (b) Interception with the consent of both parties.

The controller of the system will maintain a record of the interception exercise.

This will show:

- The system upon which the interception will occur
- The sender and the recipient, and a signed consent form from each if applicable.
- The period over which interception will be made
- The type of communication that will be intercepted and any limitations on this
- The person/s who will carry out the interception
- The reasons for the interception
- The information desired to be obtained
- The results of the interception

- (c) Interception with the consent of one party.

Any interception of communications with the consent of only one party falls under the definition of surveillance and as such should be applied for and authorised in line with the covert surveillance protocol.

The nominated Authorising officer for such interceptions will be:

- Sue Wallis, Auditor, Audit and Exchequer Section

- (d) The Council will maintain a register of all interception of communications that will have the following information:

- Date commenced
- In-house/providing assistance to an outside agency
- Level of consent
- File reference
- Date authorised – if applicable
- Date ceased

- (e) Interception without consent.

The Council is not empowered to carry out interceptions without consent. This however may change in the future, and in that event this section will be amended.

4. Procedure for interception to provide assistance to external requests.

(a) Agencies which could require assistance

There are a restricted number of agencies which can carry out interceptions without consent and who can require assistance:

- Security service
- Secret intelligence service
- GCHQ
- National criminal intelligence service
- Metropolitan police
- Police Service of Northern Ireland
- Police
- Customs and Excise
- Defence intelligence

(b) Form of request for assistance.

Where the intercepting agency requires the assistance of a communications service provider, under s11, they may serve relevant portions of their warrant on persons they consider may be able to provide such assistance or make arrangements for them to be provided.

The agency will provide the Council with the following documentation:

- A copy of the warrant instrument or relevant portion of it
Signed and dated by the Secretary of State or
Signed and dated by a senior official in cases of urgency.
- A schedule specifying:
The numbers, addresses or other factors identifying the
communications to be intercepted.
- A covering document requiring the assistance.
This will specify any other details regarding the means of interception
and delivery as may be necessary.

(c) Single point of Contact.

The Council will have a single point of contact for dealing with all such requests.

The designated officer for this role will be:

- Sue Wallis, Auditor, Audit and Exchequer Section.

8. Procedure for dealing with requests for assistance

Any member of staff when receiving a demand for assistance:.

- Pass demand to Sue Wallis.

Sue Wallis will determine if the demand is legitimate

- It comes from an authorised agency
- It has a signed and dated warrant
- It has the correct details and sufficient information to determine the interception that is requested.

Record the request

- Date received
- Requesting agency
- Interception requested.

and will determine, in consultation with relevant officers, whether:

- The Council has the ability to carry out the request
- The Council can carry out the request within the stated time scale

If not

- Inform the requesting agency of inability to comply and give reasons.
- Record the inability to comply.

If can

- Arrange for the interception to be carried out in accordance with the stated instructions.
- Disclose the intercepted material and related communication data to the requesting body.
- Continue with the interception until the warrant expires or is cancelled.
- Record the date of cessation of the interception.