

ISLE OF WIGHT COUNCIL

Covert Surveillance Policy and Procedures

Compliance

Compliance with this policy is essential because it is the only way in which Council and its staff can be protected from claims for breach of article 8 of the European Convention on Human Rights, or from vulnerability to Judicial Review of a Council decision or in any reference to the Ombudsman.

Authorisation

Only the following officers may authorise directed covert surveillance if they have received appropriate training on this policy:

Chief Executive, Director's, Head's of Service and Service Manager's

Author:	Justin Thorne
Version:	5
Status:	Final
Revision Date:	February 2010

Contents

PART A

1. Introduction
2. Relevant legislation

PART B

3. Policy
4. RIPA authorisation tests
5. Flowchart
6. Brief Guide

APPENDICES

- 1a. Application for authority to conduct directed surveillance
- 1b. Application for renewal of authority to conduct directed surveillance
- 1c. Application for cancellation of authority to conduct directed surveillance
- 1d. Review of Directed Surveillance authorisation
- 2a. Application for authorisation for CHIS
- 2b. Application for renewal of CHIS authorisation
- 2c. Review of CHIS authorisation
- 2d. Cancellation of CHIS authorisation

PART A

Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals but as a means of protecting the public from harm and preventing crime." (From the Foreword to the Home Office's Code of Practice on Covert Surveillance)

1 INTRODUCTION

- 1.1 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. Deployment of overt surveillance is increasingly commonplace in places to which the public have access and this Council has employed it in the form of CCTV and the monitoring at work policy as detailed in the Council's acceptable policy for email/internet use (Communication Policy). Any policies on either covert or overt surveillance, together with the operating procedures, systems management and documentation based on them, must take into account the requirements of the Data Protection Act 1998 (DPA) and the Human Rights Act 1998 (HRA) that must be observed in carrying out surveillance activities.
- 1.2 Advances in technology make it increasingly possible for covert surveillance to be carried out other than by CCTV techniques. Interception of communications via the Internet and telephone is now technologically possible and covert surveillance includes observation with the naked eye.
- 1.3 Covert surveillance is increasingly becoming the subject of legislative controls. The requirements of the 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. The Regulation of Investigatory Powers Act 2000 (RIPA) which came into force in October 2000 is also of relevance whenever directed covert surveillance is undertaken for the purposes of a specific investigation or operation and may result in the obtaining of private information about a person. RIPA also regulates the obtaining of communication data from a communications provider. RIPA includes a local authority within the description of public authority. Covert surveillance includes not only the use of CCTV and observation by naked eye but also the interception of communications via e-mail, the Internet, telephone or post. The use of covert human intelligence sources (CHIS) is also regulated by RIPA. A CHIS is a person who covertly establishes or maintains a relationship with someone in order to obtain information, to provide another person with access to information or to disclose information as a consequence of that relationship.
- 1.4 Covert surveillance can be either (a) intrusive, namely, carried out on any residential premises or in any private vehicle by an individual or a surveillance device on the premises or in the vehicle or (b) directed surveillance, namely surveillance undertaken covertly for the purposes of a specific investigation or operation that may result in the obtaining of private information about a person. Local Authorities are not authorised to conduct intrusive covert surveillance.
- 1.5 Council officers will at times need to conduct directed surveillance in the course of carrying out the Council's investigatory functions. It is also clear that officers will on occasions need to conduct that surveillance covertly whether the subject of the surveillance is a member of the public or a Council employee. There will also be situations where the use of a Covert Human Intelligence Source (CHIS), who can be a Council officer or member of the public, is required. All covert surveillance must be

carried out within the provisions of the relevant legislation and only commence when authorisation has been granted in accordance with this policy.

- 1.6 If any authorised Covert Human Intelligence Source (CHIS) is undertaken the Council appreciate that there may be a risk to the CHIS which needs protecting. The Council separate Whistleblowing policy in effect at the time will be followed in the interests of the protection of the informant.
- 1.7 If access is required to communication data held by a communication provider the officer must liaise with the authority's Single Point of Contact (SPOC). The Authority's SPOC is Home Office accredited and is the only person who may liaise with the communication provider to obtain the required data. No direct approach should be made by any other officer than an accredited SPOC.
- 1.8 This policy document clarifies the circumstances in which Council officers will be permitted to embark on a covert surveillance operation and the requirements that will need to be observed in order that the Council will neither contravene the relevant legislation nor the national Codes of Practice issued by the Home Office and the Office of the Information Commissioner and/or the Surveillance Commissioner. Obtaining appropriate authorisation for surveillance will be of importance to ensure that any evidence obtained is not to be judged inadmissible in any subsequent legal proceedings. Compliance with this policy also serves to avail the Council and its staff of the protection from claims for breach of article 8 HRA, or as part of a Judicial Review of a Council decision or in any reference to the Ombudsman, as it would satisfy the criteria for when interference with the rights afforded is justified.
- 1.9 If officers are at all unsure as to whether they require authorisation or if such authorisation is justified they should seek advice either from their line manager or from The Legal Team.
- 1.10 Copies of this Document and related Forms will be placed on Intranet within the Library section.
- 1.11 The Legal Team will maintain and check the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. However, it is the responsibility of the relevant authorised Officer to ensure the Legal Team receives a copy of the relevant Forms within 1 week of authorisation, review, renewal, cancellation or rejection. Where practicable, copies of the authorisation form should be sent to the Legal Team prior to authorisation to ensure that the forms are quality assured and compliant with this policy and the governing legislation.
- 1.12 Authorised officers must ensure that when sending an authorisation form to legal Services it is placed in a sealed envelope and marked private and confidential.

2.0 RELEVANT LEGISLATION

2.1 The Data Protection Act 1998

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.

2.1.2 The personal data should only be held for the purposes for which it was obtained and in all officers should be aware of the Isle of Wight Councils data protection policy which was drafted in accordance with the above principles. If an officer is unsure about their responsibilities under DPA then they should contact the Data Protection Officer.

2.2 The Human Rights Act 2000

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. It is now clear from decided cases that this right extends to activities of a professional or business nature and so includes employees. 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 Consequently, there is to be no interference with the exercise of these rights by the Local Authority under RIPA except where such interference is in accordance with the law and is necessary in a democratic society, for the purpose of preventing or detecting crime or of preventing disorder.

2.3 The Regulation of Investigatory Powers Act 2000

2.3.1 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. The interception of communications is now permitted if there is express or implied consent to the interception or where there is lawful authority for specific purposes, namely:

- (1) in order to establish the existence of facts, or to ascertain compliance with procedures applicable to the carrying out of the organisation's business, or to ascertain or demonstrate standards to be achieved or required by persons using the system;

- (2) in the interests of national security;
- (3) to prevent or detect crime;
- (4) to investigate/detect unauthorised use of the system or other telecommunications system; or
- (5) to ensure effective operation of the system.

2.3.2 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 Code of Practice and the prescribed standard forms. Authorisation for directed surveillance can be granted by the Authorising Officer of a public authority only if it is for the purposes of preventing or detecting crime or of preventing disorder until such time as the Secretary of State authorises other grounds. Those authorised officers are detailed in 3.1.3.

2.3.3 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 directed covert surveillance (of an individual) is not involved. Once surveillance becomes systematic as a means of gathering information it will be regarded as directed surveillance, RIPA will apply and the provisions of Part 2 of this document will come into effect. Similarly if the surveillance is a planned operation with a view to it being undertaken covertly, it will require authorisation. Please refer to section 4 for further guidance on the meaning of directed surveillance.

2.3.4 The act and its associated regulations also regulate the use of CHIS'. The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information as part of their normal civic duties, or to contact numbers set up to receive information e.g. Crime Stoppers or Fraud Hotline. Members of the public acting in this way would not generally be regarded as sources. A person is regarded as a CHIS if they establish or maintain a personal or other relationship with a person for the covert purpose of either; obtaining information or providing access to information to another person; or he covertly discloses information obtained by the use of the relationship or as a consequence of the existence of the relationship.

2.3.5 Authorisation for the use or conduct of a CHIS is required prior to any tasking where tasking requires the CHIS to establish or maintain a personal or other relationship for a covert purpose.

2.3.6 Material obtained from a CHIS may be used as evidence in criminal proceedings and the proper authorisation of a CHIS should ensure the legality of such evidence.

2.3.7 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.

2.3.8 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.

- 2.3.9 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 regard, throughout the use of the CHIS. The review procedure should be followed to ensure that the authorisation is still justified using the same criteria as on initial authorisation. Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled or where the investigation has been closed.
- 2.3.10 An authorisation for a CHIS may be in broad terms and highlight the nature of the CHIS's task. If this changes, then a new authorisation may need to be sought.

2.4 Confidential information

- 2.4.1 All officers should note that the only person that may authorise surveillance that may result in confidential information being obtained is the chief executive. Confidential Information includes information that may be legally privileged or health information. If any officer is unsure as to whether the investigation may information they may obtain may be confidential they should seek advice from the Legal Team.
- 2.4.2 As part of the Council's commitment to ensuring that all authorising officers are fully trained in current RIPA guidance, and to ensure that the corporate lead is appraised of current RIPA guidance, the Chief Executive shall receive regular training/updates on RIPA.
- 2.4.3 Please refer to guidance at 6.0 for guidance on what constitutes confidential information.

PART B

3 POLICY

3.1 All forms of covert surveillance

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. Consequently, directed surveillance will only be carried out for the purpose of preventing or detecting crime or of preventing disorder.

- 3.1.1 Surveillance equipment will be installed, or a CHIS used, for the above legitimate purpose only, 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. Where the subject of directed surveillance is an employee, the Head of Human Resources must be informed to ensure compliance with the Council's other relevant policies.
- 3.1.2 All requests to conduct, extend or discontinue a covert surveillance exercise or use of a CHIS must be made in writing on the forms a, b or c respectively provided in Appendix 1. All such requests must be submitted to one of the designated authorised officers who have responsibility for co-ordinating covert surveillance within the Council. All authorisations will be in writing on the appropriate forms. Authorisation will only be granted where covert surveillance or use of a CHIS is believed by the Authorising Officers or their deputies to be necessary and proportionate. Written authorisations for a covert surveillance operation will be valid for three months from the date of the original authorisation or extension subject to regular reviews of the need for such authorisation. Authorisation for a CHIS will be valid for 12 months again subject to regular reviews of the need for such authorisation.
- 3.1.3 All service managers that both undertake criminal investigations and have received appropriate RIPA training are designated as authorised officers for their own area unless they are actively involved in the specific investigation. Any team leader that does not routinely undertake criminal investigations will not be authorised until such time as they have received appropriate training or advice. Any officer senior to the designated authorising officer has authority to authorise covert surveillance or the use of CHIS. Therefore in the absence of the team leader seeking the authorisation (or if the team leader is actively part of the investigation) the Legal Services Manager, the Chief Executive Officer, the relevant Strategic Directors or the relevant Service Head may authorise the directed surveillance or use of a CHIS. The power to grant, extend and discontinue authorisations will be limited to these officers only in order to ensure greater independence and consistency.
- 3.1.4 The Council's requirements for directed 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 safe guards put in place before surveillance commences. In the event of directed surveillance needing to be carried out in an emergency, a written request and authorisation is still required using

the form at Appendix 1a. However, in an extreme situation where it is not possible for the requesting officer to complete that form, the Legal Services Manager or his deputy must be consulted. The Home Office's Code of Practice on Covert Surveillance makes provision for oral authorisation to be granted for a maximum of 72 hours in an emergency situation. A case will only be regarded as urgent if the time that would elapse before the authorising officer was available to grant the authorisation would in the **judgement of the person giving the authorisation be likely to endanger life or jeopardise the investigations or operation for which the authorisation was being given**. If the authorising officer considers the request sufficiently urgent, he or she will give oral authorisation for 72 hours. In this situation, no surveillance can commence until oral authorisation is given by the Authorising Officers or their deputies in consultation with the Legal Services Manager. Before the end of the 72 hour period authorised, the authorising officer and the applicant must meet to decide if the full period is required. If no further surveillance is required then the authority must be cancelled using the standard cancellation form. If further surveillance is required that will extend beyond the 72 hours then a renewal form should be completed, again using the standard renewal form. This subsequent authorisation will last for 3 months unless cancelled. Surveillance that is unforeseen and undertaken as an immediate response to a situation when it is not reasonably practicable to get 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. If surveillance is undertaken as a direct response to unforeseen events then authorisation will still be required if it is to continue for a sustained period. Whilst not determinative, as each should be judged on a case by case basis, the initial surveillance should not last more than 30 minutes before authority is sought. This may be either urgent authorisation or formal authorisation in line with the above policy. In no circumstance will any directed surveillance operation be given backdated authorisation after it has commenced. 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.

- 3.1.5 In circumstances where the Council's town centre CCTV overt surveillance system is to be used in a targeted-operation at the request of the Police or Customs and Excise, a Strategic Director or the Legal Services Manager, and a Police Superintendent or Customs and Excise Officer of equivalent rank will authorise such activities using an abridged version of the forms contained in the Appendix to this document. However this will only require one authorisation to be completed, usually by the police.
- 3.1.6 Surveillance equipment will only be installed with the 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 in section 4 have been considered. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant.
- 3.1.7 Audio or video recording in order to provide evidence about anything taking place on residential premises, it is to be regarded as intrusive surveillance. Such activity should not be undertaken and will not be authorised, because the effect of such surveillance is, arguably, to put the person undertaking it in the same position as if they were on the premises under surveillance.

- 3.1.8 All authorising officers will retain securely in accordance with Data Protection Act 1998 and in accordance with the Council's retention policy the originals of all authorisation documents and maintain a register of all requests and authorisations for covert surveillance together with the reasons for any request being denied (Appendix 2). All new authorisations will be reported to the Council's Data Protection Officer for his consideration whether they amount to new uses requiring registration under the DPA.
- 3.1.9 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.
- 3.1.10 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 Legal Services Manager and the Authorising Officers concerned. The Legal Services Manager 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). Separate arrangements in respect of the Council's CCTV operations for the security and review of information and access to it will apply.
- 3.1.11 A register will be maintained by all authorising officers of all reviews of material recorded and collected covertly. The reviews shall by default be reviewed monthly from the date of authorisation. The reviewing officer shall be the authorising officer. The reviewing officer should ensure that the original justification for the grant of the authorisation is still valid and must consider whether the RIPA authority is still required in accordance with section 4. A copy of the reviewing form shall be sent to the Legal Team for central record. However authorising Officers are advised as a matter of best practice to review the authorisations on a weekly basis to ensure they are still necessary. Separate arrangements in place in respect of the Council's CCTV operations will apply.
- 3.1.12 Only high-quality video and audio tapes will be used and for a maximum number of twelve times. All video and audio tapes will be identified uniquely and erased prior to reuse. 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 reused before being destroyed.
- 3.1.13 Once directed surveillance 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 or, if appropriate, the police must be involved immediately to ensure that evidential procedures and the requirements of current legislation are observed.
- 3.1.14 Copies of all authorisations to conduct, renew, review or discontinue any covert surveillance will be sent to the Legal Services Manager promptly and in any event within 1 week. Officers must be aware of the importance of maintaining the central record for quality control and audit purposes. In addition, it is advisable that the form is sent to the Legal Team prior to authorisation to ensure quality assurance.

3.1.15 Any failure to comply with this policy may be a disciplinary offence.

3.1.16 A CHIS authorisation will not be authorised unless appropriate arrangements are in place that satisfy the requirements of legislation. Appropriate arrangements must include-

(a) that there will at all times be an officer who will have day-to-day responsibility for dealing with the source on behalf of the Council, and for the source's security and welfare;

(b) that there will at all times be another officer the Council who will have general oversight of the use made of the source;

(c) that there will at all times be an officer within the Council who will have responsibility for maintaining a record of the use made of the source;

(d) that the records relating to the source that are maintained by the Council will always contain particulars of all such matters (if any) as may be specified paragraph in regulations made by the Secretary of State; and

(e) that records maintained by the Council that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

3.1.17 The authorising officer will have regard to the current code of practice for the time being in force.

3.2 Interception of Telephone Calls

3.2.1 The Council has no current facility to intercept all incoming or outgoing telephone calls to monitor and record conversations. Subscribers to the Wightcare Services' Lifeline are advised in writing when they join the scheme that their calls will be recorded. Since anyone using this facility with the subscriber's permission can be regarded as giving implied consent to the call being monitored and recorded, this surveillance can be regarded as overt.

3.2.2 The Council will also continue its current practice of providing information monthly about telephone usage on a departmental basis. This information gives details of the call volume from every telephone extension and mobile phone supplied to officers and paid for by the Council and, if required, can provide a breakdown of the numbers dialled, the duration of the calls and the dates and times they were made.

3.2.3 Employees' use of the Council's telephones for private calls is already covered in separate policies and guidance. Any employee who now uses work telephones for private calls will do so in the knowledge that such usage can be monitored, as described in communications policy, and consequently implicitly consents to the removal of any expectation of privacy.

3.2.4 The Council currently operates a system of anonymous telephone monitoring in that there is a global restriction on officers being able to dial premium line numbers and to access certain known chat/sex lines. Not all officers have the international dialling facility. This policy of variable access levels for staff will continue with revisions in respect of individual officers' access to services being made as and when required by their line managers and permitted in writing at Director level.

3.3 Monitoring of the Internet and e-mail

3.3.1 The Council already has a policy on Internet use by its employees. This is the

'Acceptable Use Policy' (Communication Policy) that sets out employees' responsibilities and liabilities. A copy of this policy is currently made available to employees attending the Council's internal e-mail training course but there maybe employees with Internet and/or Intranet access who may not have attended the course nor been given a copy of the policy. The policy is available on the Council's internal Intranet site under the library section. With the increasing availability of the Intranet and internal e-mailing facilities, it is important that all employees are made aware of the policy.

- 3.3.2 The Council's current policy of restricting access to certain undesirable Internet sites will continue. This corporate policy on covert surveillance additionally introduces monitoring and recording of all Internet usage, including e-mails sent and received. During work times, the content of employees' e-mails should be restricted to matters related to their work and job descriptions. Any employee who now uses the Internet at work for private e-mails will do so in the knowledge that such usage can be monitored and consequently implicitly consents to the removal of any expectation of privacy. This implied consent extends to checking employees' e-mail in-boxes during their absence although any e-mails clearly marked as being of a non-business nature will not be opened unless for the purpose of preventing or detecting a crime.
- 3.3.3 All external recipients of e-mails from the Council will be notified by a standard disclaimer notice on all e-mails sent from Council e-mail addresses that such communications are monitored and that the Council does not endorse any content unrelated to its official business.

3.4 Further Information

- 3.4.1 Section 4 overleaf contains a brief set of guidelines to be applied in any situation to determine whether authorisation for the proposed activity should be sought. The narrative guide is followed by a flowchart that applies the same tests in an ease-of-reference format and a brief procedure is appended at annex 2.
- 3.4.2 Any enquiries about the policy should be referred to the Council's Legal Services Manager

RIPA AUTHORISATION TESTS

Authorisation will be required for a proposed activity if the answer is 'Yes' to all of the following questions.

If the answer is 'No' to any of the following questions, the proposed activity will not be entitled to protection under RIPA and authorisation will not be granted so should not be the subject of an application request.

- (1) **Is the proposed activity 'surveillance'?** The officer must decide whether the proposed activity will comprise monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording anything monitored, observed or listened to in the course of the proposed activity and whether a surveillance device will be used.
- (2) **Is it 'covert'?** The officer must decide whether the proposed activity will be carried out in a manner calculated to ensure that the target(s) will be unaware that it is or may be taking place.
- (3) **Is it 'directed'?** The officer must decide whether the proposed activity is for the purposes of a specific investigation/operation.
- (4) **Is it likely to result in obtaining private information about a person?** The officer must decide whether any private information is *likely* to be obtained. Private information includes any information a person's private or family life and, as detailed above, this may cover information of a professional or business nature. This test is different from: "Is there the faintest chance that I will obtain private information?"
- (5) **Is it a foreseen/planned response?** The officer must decide whether the proposed activity is something other than an immediate response in circumstances where it is not reasonably practicable to get authorisation. If the proposed activity has been planned in advance and not just the immediate reaction to events happening in the course of the officer's work, it is not unforeseen and requires authorisation if all the answers to questions 1 to 4 have also been 'Yes'.
- (6) **Is it proportionate?** The officer must believe the surveillance is proportionate to what it seeks to achieve. In making this judgement the officer will consider whether the information can be obtained using other less invasive methods and whether efforts are being made to reduce the impact of the surveillance on other people who are not the subject of the operation. Authorisation will not be granted if the method of investigation is excessive by relation to the seriousness of the crime that is being investigated.

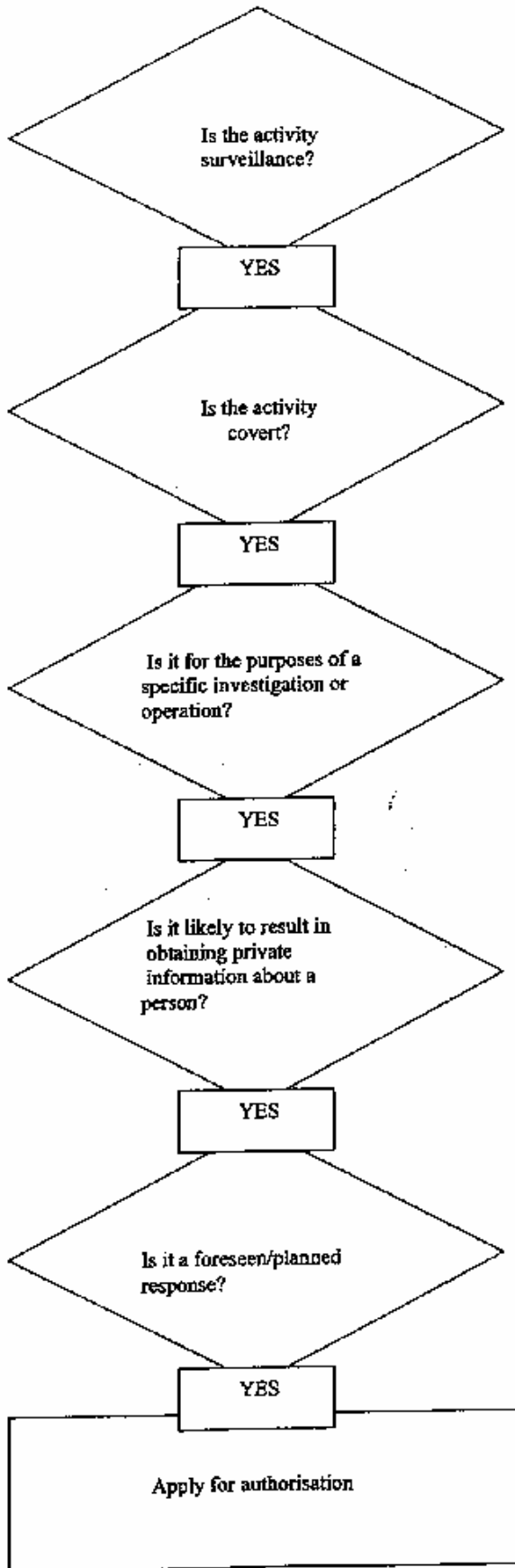
The authorising officer will not grant an authority unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation is proportionate to what is sought to be achieved by so doing. In essence is what might be discovered important enough to warrant this level of invasion. The authorising officer must balance the benefits of undertaking the investigation in the manner proposed for the public at large with the potential invasion of any persons privacy and detrimental impact this may have upon any person. The term "proportionate" is used here in the context of

the Human Rights Act which requires interference with a human right to be kept to the absolute minimum. Where there is interference it should be measured against the desired outcome. Interference with human rights is only acceptable where the matter being investigated is significant and it is in the public interest to achieve an outcome.

Covert Surveillance may in many cases involve the possibility of collateral intrusion. Authorising officers must consider whether the surveillance being authorised is undertaken with the least impact upon others who are not or will not be the subject of the investigation.

- (7) The authorising officer when deciding if the conduct is necessary if he believes that there are no overt methods of obtaining the same information for the purposes of preventing or detecting crime or of preventing disorder
- (8) Is the information Confidential? Authorising Officers must also assess the extent to which confidential information about the subject will come into the Authority's possession as a result of the investigation. Such information may be relevant to the investigation but protected for example as a result of legal professional privilege or it may be irrelevant but sensitive information for example medical records. Deliberately obtaining (or the use of) confidential information may only be authorised by the **Chief Executive** as laid down in Schedule 2 of the RIPA Act 2000.

The authorising officer must therefore be satisfied that the conduct so authorised is necessary in pursuit of a legitimate aim (no 7 above); fulfils a pressing social need and is proportionate to that aim.



If the answer to any of the above 5 questions is 'NO', RIPA protection does not attach to the planned activity and RIPA authorisation should not be applied for.

Procedure for RIPA Authorisation

This brief guide should be read in conjunction with the main policy document above.

Assessing the Application Form

Any application cannot be signed until the Authorised Officer has:

1. Taken into account this Corporate Policy & Procedures Document, any Corporate training provided and any other guidance issued, from time to time, by the Legal Team on such matters;
2. Satisfied his/herself that the RIPA authorisation is:-
 - (i) **in accordance with the law**;
 - (ii) **necessary** in the circumstances of the particular case for the purpose of **preventing or detecting crime or preventing disorder** ; and
 - (iii) **proportionate** to what it seeks to achieve.

Proportionality

In the assessment whether or not the proposed directed covert surveillance is proportionate, consideration of other appropriate means of gathering the information must be taken into account. Only **the least intrusive surveillance will satisfy the test of proportionality and be in accordance with this policy.**

Collateral Intrusion

The authorized officer must further consider the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). If such intrusion is identified then measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

Review

A date **must** be allocated for review of the authorisation. This should be 1 month from the date of the authorisation. However please note that informal reviews of the authorisation should be undertaken every week. Whilst the formal review requires completion of the review form, the informal review does not. However a record that it has been undertaken should be kept.

Central record

Ensure that any RIPA Departmental Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Legal Services Manager's Central Register, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.** In addition, it is advisable that the form is sent to the Legal Team prior to authorisation to ensure quality assurance.

CHIS

When authorising the conduct or use of a CHIS, the Authorised Officer **must also** be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

Duration

The Form **must be renewed at the time stated and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts 3 months (from authorisation)

for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent' and the forms do not automatically expire. The forms have to be reviewed, and/or cancelled and the central record at the Legal Team notified.

Confidential Information

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information is involved.

Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. So for example extra care should be given where through the use of surveillance it would be possible to acquire knowledge of discussion between the Minister of Religion and an individual relating to the latter's spiritual welfare or when matters of medical or journalistic confidentiality or legal privilege may be involved.

In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level authorisation. Only the Chief Executive may authorise the use of surveillance where it is likely that knowledge of confidential information will be acquired. Unless the matter is of extreme urgency any officer that believes that confidential information will be acquired during the surveillance should complete the standard RIPA 1 form and discuss the matter with Legal prior to submission to the Chief Executive for authorisation.

The concept of legal privilege applies to the provision of professional legal advice by any legal individual, agency or organisation qualified to do so. Legal privilege does not apply to communications made with the intention of furthering criminal purpose. Legal privilege communications will lose their protection if there are grounds to believe for example that the professional legal adviser is intending to hold or use them for a criminal purpose. The privilege is not lost if the professional legal adviser properly advising the person is suspected of having committed a criminal offence.

In general an application for surveillance which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. It will be particularly important to ensure that the proposed surveillance is necessary and proportionate under Section 28 of the Regulation of Investigatory Powers Act 2000 is satisfied. Regular reporting and review meetings should be organised to ensure that any authorisation granted is required to continue.

Similar considerations must also be given to authorisations that involve confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information which can include both oral and written communications is held in confidence but is subject to an expressed or implied understanding to hold it in confidence or it is subject to restriction on disclosure or an obligation of confidentiality contained in the existing legislation. Examples might include consultations between a health professional and a patient or information from a patient's medical record. Spiritual counselling means conversations between an individual and a Minister of Religion acting in his official capacity where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the divine being(s) of their faith.

Confidential journalistic material 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.

It is extremely unlikely that due to the nature of the surveillance the Council undertakes that confidential information will be obtained. However in order to ensure that RIPA forms are completed properly all applicants and authorising officers should ensure that if none is likely to be obtained that this is recorded within the box on the forms. If an officer is unsure as to whether a proposed investigation is likely to require any confidential information they should seek immediate advice from the Isle of Wight Council's Legal Services Section.