

St Albans City and District Council

The Regulation of Investigatory Powers Act 2000: A policy and procedure guide on the use of covert surveillance and “covert human intelligence sources”

Statement of Intent: St Albans City and District Council attaches a high value to the privacy of citizens. It will adhere to the letter and to the spirit of the Act and will comply with this Code.

POLICY

1. Introduction

- 1.1 The Regulation of Investigatory Powers Act 2000 (“RIPA”) is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that privacy is only interfered with where the law permits and there is a clear public interest justification.

2. What does RIPA do?

- 2.1 RIPA places controls on the use of certain methods of investigation. In particular, it regulates the use of surveillance and “covert human intelligence sources”. This guide covers these aspects of the Act. Further guidance will be issued on other aspects of the Act if necessary.
- 2.2 RIPA’s main implications for the Council are in respect of covert surveillance by Council officers and the use of “covert human intelligence sources”. (A covert human intelligence source is someone who uses a relationship with a third party in a secretive manner to obtain or give information – for instance an informer or someone working “under cover”.)

3. Some definitions

3.1 “Covert”

Concealed, done secretly

3.2 “Covert surveillance”

Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

3.3 *“Directed surveillance”*

Directed surveillance is defined in RIPA as surveillance which is covert, but not intrusive, and undertaken:

- a) for the purposes of a specific investigation or operation;
- b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance (i.e. where the circumstances make it impractical to seek authorisation. An example might be where an officer on patrol or carrying out other duties sees a person acting suspiciously and decides to watch them surreptitiously to see whether they are intending to commit a crime.)

Private information in relation to a person includes any information relating to his private or family life.

3.4 *“Intrusive surveillance”*

Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

- a. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

4. RIPA and Surveillance – what is not covered

- 4.1 General observation forms part of the duties of some Council officers. They may, for instance, be on duty at events in the City and District and will monitor the crowd to maintain public safety and prevent disorder. Environmental Health Officers might covertly observe and then visit a shop as part of their enforcement function. Such observation may involve the use of equipment merely to reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of RIPA.

- 4.2 Neither do the provisions of the Act cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. (There is a separate Code of Practice adopted by the Council to govern use of CCTV.

5. RIPA and Surveillance – What is covered?

- 5.1 The Act is designed to regulate the use of “covert” surveillance. Covert surveillance means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. Strictly speaking, only two types of covert surveillance are regulated by RIPA – “directed” and “intrusive” surveillance. However, where the purpose of a surveillance operation is to obtain private information about a person, the authorisation procedures set out in this guide should be followed and the surveillance treated as being “directed”.

6. What is “directed surveillance”?

- 6.1 Directed surveillance is defined in RIPA as surveillance which is covert, but not intrusive, and undertaken:
- a) for the purposes of a specific investigation or operation;
 - b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
 - c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance. (See the clarification of this in paragraph 3.3.)

Private information in relation to a person includes any information relating to his private or family life.

- 6.2 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person’s life, activities and associations. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a plain clothes police officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of a patrol.
- 6.3 Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. Such activity is defined as “intrusive surveillance” and is dealt with in paragraph 7.

- 6.4 In practice, the sort of directed surveillance which the Council might undertake would include the use of concealed cameras as part of an investigation into antisocial behaviour. It might include covert surveillance connected with the prosecution of environmental health offences or effective planning enforcement notices or in connection with investigating benefit fraud. You should treat anything involving the use of concealed cameras or anything involving keeping covert observation on premises or people as potentially amounting to directed surveillance. If you are unsure, please take advice either from your manager or supervisor, or from the Head of Legal and Democratic Services.
- 6.5 Directed surveillance **must** be properly authorised in accordance with the procedure set out in section 9.
- 6.6 You should treat any covert surveillance which is likely to intrude upon anyone's privacy to more than a marginal extent as directed surveillance, even if it does not fall within the strict terms of the definition – for instance where surveillance is not part of a specific investigation or operation.

7. What is intrusive surveillance?

7.1 An important warning: the Council cannot authorise intrusive surveillance.

- 7.2 Intrusive surveillance is defined as covert surveillance that:
- a. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
 - b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.
- 7.2 In essence, intrusive surveillance amounts to intrusion into people's homes or vehicles either physically or by means of a surveillance device.
- 7.3 **Intrusive surveillance cannot be undertaken without authorisation and the Council cannot authorise intrusive surveillance.** Bodies such as the Police and Customs and Excise can authorise intrusive surveillance. If you are asked by another agency to co-operate with intrusive surveillance, you should seek advice from the Head of Legal and Democratic Services immediately. Where other authorities say that they are authorised to undertake intrusive surveillance but need our co-operation, we need to check that their authorisation is in order.

8. What is a covert human intelligence source?

- 8.1 A covert human intelligence source is someone who establishes or maintains a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informer or Council

officer to strike up a relationship with someone as part of an investigation to obtain information “under cover”.

- 8.2 Someone who volunteers information to the Council, either as a complainant (for instance, about anti-social behaviour or a breach of planning regulations) or out of civic duty, is unlikely to be a covert human intelligence source. If someone is keeping a record, say, of neighbour nuisance, this will not amount by itself to use of a covert human intelligence source. However, if we are relying on, say, a neighbour to ask questions with a view to gathering evidence, then this may amount to use of a covert human intelligence source.
- 8.3 The use by the Council of covert human intelligence sources is expected to be extremely rare and, for that reason, this guide does not deal with the issues to which they give rise. If you are contemplating use of a covert human intelligence source, please take advice from the Head of Legal and Democratic Services before putting your plan into action.

9. Authorising Directed Surveillance: The Rules

- 9.1 It is crucial that all directed surveillance is properly authorised. Failure to secure proper authorisation and to comply with this procedure could lead to evidence being excluded by the courts and to complaints against the Council. The Council is subject to audit and inspection by the Office of the Surveillance Commissioner and it is important that we can demonstrate compliance with RIPA and with this code. **Again, please note that the Council cannot authorise intrusive surveillance – see section 7.**
- 9.2 **Who can authorise directed surveillance?** Regulations made under the Act say that the most junior level at which authorisations can only be given is by what it refers to as “assistant chief officers”. For the purposes of this Code, authorisations may only be given by the officers identified in the Appendix to this Guide referred to as “authorising officers”. In cases of urgency, if it is not possible to seek authority from an authorising officer, authority may be given by a deputy to an authorising officer, but ratification of that authority should be sought at higher level as soon as practical, and the reasons for urgency recorded on the authorisation form. Where practical, the authorising officer should not be directly involved in the case giving rise to the request for authorisation. (However, an authorising officer may authorise a request made by staff who report to them if they are not directly involved in the case.) Where it is not practical for authorisation to be given by an officer who is not directly involved, this should be noted with reasons on the authorisation form.
- 9.3 **On what grounds can directed surveillance be authorised?** Directed surveillance can only be authorised by local authorities:

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

(When the legislation was introduced, the Council could authorise directed surveillance on other grounds (e.g. in the interests of public safety or in the

interests of protecting public health) but the crime and disorder ground is the only one available to local authorities. The Police have wider powers to authorise directed surveillance.)

Please note that surveillance has to be **necessary** for the crime and disorder purpose. If you can just as well carry out an investigation by means which do not involve directed surveillance, then you should use them.

- 9.4 **Is the proposed surveillance proportionate?** Authorisation should not be sought, and authority should not be given unless you are satisfied that the surveillance is proportionate. You should make sure that any interference with privacy is justified by the end being sought. If the benefit to be obtained from surveillance is marginal, or if the problem you are seeking to tackle is not very serious, you should think very carefully about whether the use of surveillance is proportionate. We should not “use a sledgehammer to crack a nut”!
- 9.5 **Is the proposed surveillance discriminatory?** The Council is under a legal obligation to avoid either direct or indirect discrimination in carrying out its functions. As surveillance can interfere with rights contained in the European Convention on Human Rights, discrimination can also amount to a breach of the Human Rights Act. You should be sensitive to this issue and ensure that you apply similar standards to seeking or authorising surveillance regardless of ethnic origin, sex or sexual orientation, disability, age etc. You should be alert to any assumptions about people from different backgrounds which may not even be consciously held.
- 9.6 **Might the surveillance involve “collateral intrusion”?** In other words, might the surveillance intrude upon the privacy of people other than those who are the subject of the investigation. You should be sensitive of the privacy rights of third parties and consider very carefully whether the intrusion into their privacy is justified by the benefits of undertaking the surveillance.
- 9.7 **Might the surveillance involve acquiring access to any confidential or religious material?** If so, then the surveillance will require a particularly strong justification and arrangements need to be put in place to ensure that the information obtained is kept secure and only used for proper purposes. Confidential material might include legal or financial records, or medical records. Where there is a possibility that access to confidential or religious material might be obtained, the authorisation of the Chief Executive should be sought.
- 9.8 Any authorisations when knowledge of confidential information is likely to be acquired must be authorised by the Chief Executive or in his absence his deputy.

PROCEDURE

10. Authorising Directed Surveillance: The Procedure

10.1 Applying for authorisation.

10.1.1 Applications for authorisation must be made on the correct form, except in case of extreme urgency, in which case written authorisation should be sought at the earliest opportunity. The form to seek authorisation is reproduced at Appendix 2 to this Guide. It, and other forms and information, may also be found on the Home Office web site at www.homeoffice.gov.uk (see Appendix 6)

10.1.2 A written application for authorisation for directed surveillance should describe in detail any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

10.1.3 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given; and/or

- the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

10.1.4 Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

10.2 Duration of authorisations

10.2.1 A written authorisation granted by an authorising officer will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

10.2.2 Urgent oral authorisations or written authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after **seventy-two hours**, beginning with the time when the authorisation was granted or renewed. This will apply to written authorisations given by deputies to Heads of Services.

10.2.3 Even though authorisations cease to have effect after three months, you should not simply leave them to run out. When the surveillance ceases to be necessary, you should always follow the cancellation procedure. See section 10.5. Where surveillance has ceased, we must be able to match each authorisation with a cancellation.

10.3 Reviews

10.3.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The maximum period between authorisation and review, and between reviews, should be four weeks. The more significant the infringement of privacy, the more frequent should be the reviews. The results of a review should be recorded on the central record of authorisations (see paragraph 11). Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

10.3.2 In each case authorising officers within the Council should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

10.3.3 The form to record a review of an authorisation is reproduced at Appendix 3 to this Guide.

10.4 Renewals

10.4.1 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, s/he may renew it in writing for a further

period of **three months**. A single renewal may also be granted orally in urgent cases and may last for a period of **seventy-two hours**.

10.4.2 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations (other than oral authorisations in urgent cases) may be renewed more than once, provided they continue to meet the criteria for authorisation.

10.4.3 All applications for the renewal of an authorisation for directed surveillance should be made on the form attached as Appendix 4 to this guide and should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information given in the original application for authorisation;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

10.4.4 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations (see paragraph 12).

10.5 Cancellations

10.5.1 The authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer. If in doubt about who may cancel an authorisation, please consult the Head of Legal and Democratic Services. Cancellations are to be effected by completion of the form in Appendix 5 to this Guide.

10.5.2 **N.B. Please note the warning in paragraph 10.2.3 that there must be a completed cancellation for each authorisation once surveillance has been completed. An authorisation cannot simply be allowed to expire.**

10.6 Ceasing of surveillance activity

10.6.1 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be included in the Notification of Cancellation form.

11. Record Keeping and Central Record of Authorisations

11.1 In all cases in which authorisation of directed surveillance is given, the Service Head is responsible for ensuring that the following documentation is kept safely for a period of at least three years from the date of authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the authorising officer.

11.2 In addition, copies the following must be sent to the Head of Legal and Democratic Services immediately upon completion:

- all completed forms authorising directed surveillance;
- the Head of Legal and Democratic Services will then allocate the authorisation with a unique reference number
- all completed forms authorising renewal of directed surveillance;
- all completed forms cancelling directed surveillance.

These will be kept by the Head of Legal and Democratic Services who is also the Monitoring Officer who will review them at least every twelve months.

12. Authorising Use of Covert Human Intelligence Sources

12.1 Similar principles and procedures apply to authorising the use of covert human intelligence sources. If it becomes apparent that their use is more than very exceptional, detailed guidance will be published and circulated. For the present, officers' attention is drawn to the explanation of the nature of a covert human

intelligence source in Paragraph 9. If you think you might be using, or might use, a covert human intelligence source, please contact the Head of Legal and Democratic Services, who will advise on the principles to be applied, the authorisation procedure, record keeping etc. For the avoidance of doubt, the Council will comply, so far as applicable, with the model guidance issued by the Home Office.

13. Access to Communications data

- 13.1 There are stringent controls placed on access by the Council to “communications data”. The Council is not entitled to obtain access to the content of communications between third parties but can, in some circumstances, obtain information relating to the use of a communications service. “Communications services” include telecom providers, postal services and internet service providers.
- 13.2 This is a complex area, procedurally and legally. Access to communications data can only be obtained through the Council’s designated “single point of contact” (“SPOC”) for communications data. At the present time we do not actually exercise these powers as we do not have a designated “SPOC”.

14. Further Information

- 14.1 There is much helpful information on the Home Office web site about RIPA. See www.homeoffice.gov.uk (see Appendix 6)
- 14.2 The Head of Legal and Democratic Services is happy to advise further on issues connected with RIPA. Departments need to consider what their training needs are in this area. Regular training courses are arranged to keep officers up to date.

Michael Lovelady
Head of Legal & Democratic Services and Monitoring Officer

Appendices

Appendix One: Authorising Officers under Regulation of Investigatory Act 2000.

Appendix Two: Form for Authorising directed covert surveillance.

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/application-directed-surveillanc?view=Standard&pubID=447375>

Appendix Three: Form for Review of authorisation for directed covert surveillance.

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/review-directed-surveillance?view=Standard&pubID=447381>

Appendix Four: Form for Renewal of authorisation for directed covert surveillance.

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/renewal-directed-surveillance?view=Standard&pubID=447379>

Appendix Five: Form for Cancellation of authorisation for directed covert surveillance.

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/cancellation-directed-surveillan?view=Standard&pubID=447377>

Appendix Six: Links to various information on Home Office Website

<http://www.homeoffice.gov.uk/> and Flow Chart showing links to the Acts, Codes of Practice and the Forms.

Home



Advance Search



RIPA Forms or RIPA Codes of Practice

Appendix One: Authorisation of Officers under Regulation of Investigatory Powers Act 2000

I hereby approve the following as designated officers under the Regulation of Investigatory Powers Act 2000 to give authorisations for directed covert surveillance and the use of a covert human intelligence source:-

Head of Planning and Building Control Services
Head of Housing
Chief Policy and Partnerships Officer
Head of Human Resources, Customer Services and IT
Head of Legal Democratic and Regulatory Services and Monitoring Officer
Chief Finance Officer
Head of Community Services
Legal Services Manager and Deputy Monitoring Officer

Daniel Goodwin
Chief Executive

March 2011