

SEVENOAKS DISTRICT COUNCIL

SURVEILLANCE POLICY

The Regulation of Investigatory Powers Act 2000

INTRODUCTION

1. The Regulation of Investigatory Powers Act 2000 (RIPA) is in force to ensure that relevant investigatory powers are used in accordance with the Human Rights Act 1998 (HRA) and The Data Protection Act 1998 (DPA). RIPA sets out a statutory framework for the granting of authority to carry out surveillance.
2. Covert surveillance is surveillance that is carried out in a manner to ensure that the persons subject to the surveillance are unaware that it is taking place. Covert surveillance can be either:
 - Intrusive Surveillance
 - Directed Surveillance
3. Intrusive Surveillance is 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. Although 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 or in the premises or vehicle.
4. Directed Surveillance is covert but not intrusive and is undertaken
 - for the purposes of a specific investigation or operation;
 - 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 purpose of the investigation or operation);and
 - 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 to be sought for the carrying out of surveillance.
5. The main area that the Council is concerned with is Directed Surveillance and the Act identifies an authorisation process prior to the commencement of any investigation.
6. Local authorities are not authorised to conduct Intrusive Surveillance.
7. The use of covert human intelligence sources (CHIS) is also regulated by RIPA. A CHIS is a person who establishes or maintains a relationship with someone in order to covertly obtain information, to provide another person with access to information or to disclose information as a result of that relationship.
8. This Policy document sets out the circumstances in which Council Officers will be permitted to undertake a covert surveillance operation and the requirements that will need to be observed in order that the Council does not

contravene relevant legislation or the national Codes of Practice issued by the Home Office and the Office of the Information Commissioner.

The Legislation

9. The DPA provides that personal data, which includes personal data obtained from covert surveillance techniques must:
 - be fairly and lawfully obtained and processed;
 - be processed for specified purposes and not in any manner incompatible with those purposes;
 - be adequate, relevant and not excessive;
 - be accurate
 - not be kept for longer than is necessary;
 - be processed in accordance with individuals' rights;
 - be secure;
 - not be transferred to non-European Economic Area countries without adequate protection
10. Article 8 of the European Convention on Human Rights is relevant in respect of covert surveillance as everyone has the right to respect for his/her private and family life, home and correspondence. In addition, Article 6 is of relevance in relation to covert surveillance as everyone has the right to a fair trial, including internal procedures or hearings and this principle of fairness extends to the way evidence is obtained.
11. RIPA ensures that the individual rights and freedom are protected when carrying out effective law enforcement.
12. 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 associated regulations if such surveillance has been authorised in the manner provided by the Act. Authorisation for Covert Surveillance can be granted by the Authorising Officer of a local authority if it is for the purposes of preventing or detecting crime or preventing disorder:

Authorisation

13. Authorising Officers are designated as follows:-
 - Head of Development Services;
 - Head of Environmental & Operational Services;
 - Head of Information and Customer Services;

- Head of Housing Services;
- Head of Finance and Human Resources;

together with all more senior officers within the Authority.

Ideally, Authorising Officers should not be responsible for authorising their own activities, i.e. those operations/investigations in which they are directly involved. However, it is recognised that this may sometimes be unavoidable especially where it is necessary to act urgently.

14. Applications for authority for directed surveillance or the use of a CHIS must be made in writing to an Authorising Officer using the appropriate application form(s) shown at Appendix 1. In urgent cases an authorisation may be given orally, but such authorisation must be confirmed in writing using the appropriate application form as soon as is reasonably practicable.

Content

15(a). The application for authorisation for directed surveillance shall record:

- the purpose of the specific operation or investigation
- the grounds on which the directed surveillance is necessary e.g. for the prevention or detection of crime, and why the surveillance is necessary on the identified grounds;
- why the directed surveillance is considered to be proportionate to what it seeks to achieve (here, it should be explained what suspicions and/or existing evidence merit continued investigation, what other means of gathering sufficient information have been tried or considered, and therefore why directed surveillance is now the required course of action);*
- the identities, where known, of those to be the subject of directed surveillance (this may include descriptions of physical appearance);
- a detailed description of the surveillance proposed to be undertaken (this should include, for example, the location(s) (including any premises, equipment or vehicles involved) times, method(s), personnel involved);
- an explanation of the information which it is desired to obtain as a result of the authorisation;
- an assessment of the risk of any collateral intrusion or interference affecting any person(s) other than the subject(s) of the directed surveillance, and an explanation of how this will be minimised;**
- dates for the regular reviews of the authorisation;
- whether it is likely that knowledge of confidential information will be acquired. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic

material. In such a situation a higher level of authorisation is needed being the Head of Paid Service or in his/ her absence a Director; ***

- the authorising officer should spell out the '5 Ws' i.e. who, what, where, when, why and how. In particular, they should state why they believe the directed surveillance is necessary, and why they believe it is proportionate to what is sought to be achieved by carrying it out
- for "urgent" cases, a subsequent explanation of why the case was considered to be so urgent that an oral instead of written authorisation was given and/ or why it was not reasonably practicable to seek prior authorisation from the authorising officer;
- details of the applying officer and of the Authorising Officer;
- the date/time from which the authorisation comes into effect, and the expected duration.
- Each authorisation must be uniquely numbered using the number sequence from the Council's central record. The officer applying for authorisation must ensure they have obtained the next available sequential number from the Monitoring Officer before submitting the form for authorisation.

* There is a need to balance the intrusiveness of the activity on the targets and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by less intrusive means. All such activity should be carefully managed to meet the objectives and must not be arbitrary or unfair.

** Those carrying out covert surveillance should inform the Authorising Officer if the investigation/operation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation/operation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

*** Authorising Officers must pay particular attention to the risks of collateral intrusion or obtaining confidential material in order to ensure that proportionality is observed and the product is protected.

15.(b) The application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS) shall record

- How will the source be referred to i.e. pseudonym or reference number;
- Details of the person within the authority ('the controller'), who will have general oversight of the use made of the source;

- Details of the person responsible for retaining (in secure, strictly controlled conditions, with need to know access), the source's true identity, a record of the use made of the source and the particulars required under the RIP (Source Records) Regulations 2000;
- The purpose of the specific operation or investigation;
- The purpose for which the source will be tasked or used;
- Details of the proposed covert conduct of the source or how the source is to be used;
- The grounds upon which the use of the source is necessary, and why the use of the source is necessary on the identified grounds;
- Details of any potential collateral intrusion and why this is unavoidable, together with details of any precautions to be taken to minimise this intrusion;
- Details of any particular sensitivities in the local community where the source is to be used; Any other similar activities being undertaken by public authorities that could impact on the use of the source;
- An assessment of the risk to the source in carrying out the proposed conduct;
- Why the conduct or use of the source is proportionate to what it seeks to achieve;
- whether it is likely that knowledge of confidential information will be acquired. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. In such a situation a higher level of authorisation is needed being the Head of Paid Service or in his/ her absence a Director; **
- the authorising officer should spell out the '5 Ws' i.e. who, what, where, when, why and how. In particular, they should state why they believe the conduct or use of the source is necessary, and why they believe such conduct or use is proportionate to what is sought to be achieved by the engagement of the source
- dates for the regular reviews of the authorisation;
- for "urgent" cases, a subsequent explanation of why the case was considered to be so urgent that an oral instead of written authorisation was given and/ or why it was not reasonably practicable to seek prior authorisation from the authorising officer;
- details of the applying officer and of the Authorising Officer;

- the date/time from which the authorisation comes into effect, and the duration.
- Each authorisation must be uniquely numbered using the number sequence from the Council's central record. The officer applying for authorisation must ensure they have obtained the next available sequential number from the Monitoring Officer before submitting the form for authorisation.

** Authorising Officers must pay particular attention to the risks of collateral intrusion or obtaining confidential material in order to ensure that proportionality is observed and the product is protected.

Review

16. Authorising Officers are also responsible for carrying out regular reviews of applications which they have authorised including the review of a CHIS. Such reviews should take place as frequently as is considered necessary and practical. The appropriate form(s) shown at Appendix 2 should be completed.

It is recommended that the Authorising Officer will require reviews to be conducted at intervals of not longer than one month for Directed Surveillance and three months for a CHIS.

Duration and Renewals

17. A written authorisation 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. In the case of a CHIS the written authorisation will cease to have effect (unless renewed) at the end of a period of twelve months beginning on the day on which it took effect.

Urgent oral authorisations, if not already ratified in a written authorisation, will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

18. If at any time before an authorisation would cease to have effect, the Authorising Officer agrees it is necessary for the authorisation to continue for the purpose for which it was given, he/she may renew it in writing for a further period of three months, beginning with the day when the authorisation would have expired but for the renewal. In the case of a CHIS this may be renewed in writing for a further period of twelve months. Applications for the renewal of an authorisation for directed surveillance, or renewal of a CHIS must be made on the appropriate renewal request form(s) shown at Appendix 3.
19. All applications for the renewal of an authorisation for directed surveillance should record:
- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

- the information as appropriate at 15 above, as it applies at the time of the renewal;
- any significant changes to the information in the previous authorisation;
- the reasons why it is necessary to continue the 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

Cancellations

20. An Authorising Officer must cancel an authorisation if he/she becomes satisfied that the surveillance is no longer required or appropriate.
21. Cancellations for directed surveillance or a CHIS must be made using the appropriate cancellation form(s) shown at Appendix 4.

Registration

22. The Council's Monitoring Officer will be responsible for monitoring authorisations and carrying out an annual review of authorisations, reviews, renewals, refusals and cancellations.
23. Authorising Officers will retain 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. All new authorisations will be reported to the Council's Data Protection Officer for consideration as to whether they amount to new uses requiring registration under the DPA.
24. All authorisations, reviews, renewals, refusals and cancellations must be promptly copied to the Monitoring Officer along with reasons for refusals, who will maintain a central register of all cases of covert surveillance undertaken by investigation sections of Sevenoaks District Council. These documents will form part of the central register.

RIPA authorisation forms and any information collected by means of covert surveillance should be retained securely for a period of five years after which time the Authorising Officer must review whether the information should be disposed of or retained for a further length of time. The Authorising Officer should take into consideration the status of any legal proceedings connected to the operation and the likelihood of any future legal action (including action taken by the subject(s) of the surveillance). The reasons for any decision to keep the information for longer than 5 years must be documented and retained with the file. Authorising Officers must not grant authorisation for covert surveillance unless the following have been documented

- The officer who will be responsible for retaining the information and disposing of the same in a secure manner;

- The physical, technical and organisational measures that have been put in place to prevent unauthorised access to and use of the information obtained by the surveillance exercise;
- The physical, technical and organisational measures that have been put in place to prevent accidental or unauthorised loss of the information obtained by the surveillance exercise;

Matters to be considered by the Authorising Officers

25. 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 use of overt means should always be considered. If this is not feasible the reason should be given.
26. The Council's requirements for covert surveillance will normally be carefully planned so that the necessary consultancy regarding work assessment, insurance and health and safety can be carried out and the required priorities put in place before surveillance commences.
27. 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.
28. 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.
29. 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.
30. Covert surveillance equipment will only be installed with the necessary authorisation of the Council's Authorising Officer. 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. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant. The authorising officer must evaluate whether the use of covert surveillance equipment does not become intrusive surveillance which the Council is not authorised to conduct (see paragraph 3).

Any request by a Council Officer to a resident to keep a video/audio/written diary as part of a covert evidence gathering exercise will be regarded as a covert surveillance exercise conducted on behalf of the Council and must be authorised according to the procedures set out in this policy document.

31. If a CCTV camera or video camera is to be used, the Authorising Officer must make himself familiar with the product of the surveillance so that he can see if any sensitive material has been captured in order to avoid its publication.
32. The Council may be asked to act on behalf of another, such as a national body in a covert surveillance operation. In addition, the Council itself may use an outside contractor to carry out covert surveillance on its behalf. In either case, it is the principal which issues the authorisation and ensures that the Agent is aware of the scope of the operation, its detailed methodology and its ultimate cancellation. It is the Authorising Officer's responsibility to ensure that this is communicated to the Agent and that the Agent reports back to the Authorising Officer as and when necessary as prescribed by the Authorising Officer.

Examples of when an Authorisation is needed for Directed Surveillance or CHIS

33. Examples of areas of work in which officers may require authorisation are as follows:-
 - Revenues and Benefits – benefit fraud
 - Planning and Building Control – breach of Enforcement Notices, Breach of Condition Notices, other planning offences
 - Highways
 - Environmental Services – breach of Abatement Notices, health and safety breaches, hackney carriage offences, public entertainment licensing, fly tipping.
34. If an investigation is being considered, then an authorisation should be obtained if it is the intention not to advise the suspect that his/her activities will be observed.
35. Overt surveillance does not require any RIPA authorisation. Therefore 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. Registered Post should be used in such circumstances and all letters and other communications should only last for a maximum of 3 months.
36. CCTV systems are normally not within the scope of RIPA since they are overt and not being used for a specific operation or investigation. However where CCTV is used as part of a pre-planned operation of surveillance then authorisation should be obtained, setting out what is authorised, how it will be carried out, that is which cameras are to be used, and what activity is to be caught and held on the tape or disc that results. Control room staff should ensure that they understand the terms of the authorisation and Authorising Officers must notify them of changes. (see paragraphs 30, 31 and 32)
37. Certain levels of surveillance amounting to general observation in the course of law enforcement can be regarded as "low level" surveillance 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 complied with. However, if Officers revisit the site this would be regarded as systematic and RIPA authority will be required. In addition, Directed Surveillance does not include covert surveillance carried out by way of an immediate response to events which by their nature could not have been foreseen. Therefore emergency call outs to the Duty Liaison Officers are not included.

Complaints

38. RIPA establishes an independent Tribunal. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

Details of the relevant complaint procedure can be obtained from the following address:

Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

Policy Availability

39. This policy will be published in accordance with the Council's publication scheme under the Freedom of Information Act 2000.

Is the activity
Surveillance?



Is it Covert?

If not no need to apply for
RIPA authority



Is it intrusive?

If YES, it cannot be
authorised



If not Intrusive does it
involve a CHIS?

If YES



If no CHIS is it:

1. For the purpose of a specific investigation or operation?
2. Likely to result in obtaining private information about a person?
3. Foreseen/planned response.

If the answer to all 3 questions is YES, apply for authorisation for DIRECTED SURVEILLANCE.

If the answer to any question is NO, RIPA protection does not attach and proposed surveillance could be unlawful

1. Can you answer YES to the 3 questions relating to DIRECTED SURVEILLANCE?
2. Have you considered the vulnerability of the CHIS?
3. Are resources available to appoint a Handler and a Controller of the CHIS.

If the answer to all questions is YES, apply for authorisation for a CHIS.

If the answer to any question is NO, RIPA protection does not attach and proposed surveillance could be unlawful.

APPENDIX 1

Forms

- Application for Authorisation to Carry Out Directed Surveillance
- Application for Authorisation of the use or Conduct of a Covert Human Intelligence Source (CHIS)

The forms are available via the Home Office website
<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/>

APPENDIX 2

Forms

- Review of a Directed Surveillance Authorisation
- Review of a Covert Human Intelligence Source (CHIS) Authorisation

The forms are available via the Home Office website
<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/>

APPENDIX 3

Forms

- Application for Renewal of a Directed Surveillance Authorisation
- Application for Renewal of a Covert Human Intelligence Source (CHIS) Authorisation

The forms are available via the Home Office website <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/>

APPENDIX 4

Forms

- Cancellation of a Directed Surveillance Authorisation
- Cancellations of an Authorisation For the Use or Conduct of a Covert Human Intelligence Source

The forms are available via the Home Office website <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/>