

WEALDEN DISTRICT COUNCIL

POLICY AND GUIDANCE ON THE
REGULATION OF INVESTIGATORY POWERS ACT
2000

Introduction

1. The Regulation of Investigatory Powers Act 2000 ("RIPA") regulates the work of the council relating to surveillance, the use of covert human intelligence sources ("CHIS") and the accessing of certain communications data through a single point of contact (SPOC). It provides a legal framework for authorising investigations in a manner consistent with obligations under the Human Rights Act 2000 ("HRA") where the investigation is for the purposes of preventing or detecting crime or for preventing disorder.
2. RIPA is wide ranging in its application and will impact all officers with an enforcement or investigatory capacity, including internal investigations. Failure to comply with RIPA may result in a claim for a breach of the HRA. This may result in evidence being deemed inadmissible in a prosecution or even a claim for compensation for an infringement of that person's human rights.
3. The Council is committed to implementing RIPA in a manner that is consistent with the spirit and letter of RIPA and the HRA. The Council is committed to conducting all relevant actions in a manner which strikes a balance between the rights of the individual and the legitimate interests of the public.

Codes of Practice

4. Statutory Codes of Practice supplement RIPA. These deal respectively with covert surveillance, CHIS, interception of communications, communications data and electronic information. They are available on the following web link:

[:http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/](http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/)

5. The Council's policy recognises the important role these Codes of Practice play in the practical implementation of RIPA. The Council will conduct all of its activities relating to RIPA whilst having due regard to and whilst following the recommended practice of the Codes of Practice. It is essential, therefore, that all relevant officers involved in RIPA are familiar with the content of these Codes of Practice.

Surveillance

6. Covert surveillance is defined in section 26(9)(a) of RIPA as any 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. It may be either direct or intrusive surveillance.

7. Directed surveillance is defined in section 26(2) of RIPA as surveillance which is covert, but not intrusive, and undertaken:
 - a. for the purposes of a specific investigation or specific 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 Part II of RIPA to be sought for the carrying out of the surveillance.

8. Intrusive surveillance is defined in section 26(3) of RIPA 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.

9. Local Authorities are NOT authorised to conduct Intrusive Surveillance.

10. A CHIS is defined in section 28(8) of RIPA as a person who:
 - a. establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling with paragraph (b) or (c);
 - b. he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
 - c. he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

Communications Data

11. In addition to carrying out covert surveillance and the use of a CHIS, the Council may also access certain communications data under RIPA, provided this, like all other surveillance, is **for the purpose of preventing or detecting crime or of preventing disorder**.

12. Authorisations may be granted by a Designated Person, who shall seek the advice of the Council's SPOC (Single Point of Contact) authorised by the Home Office. The codes of practice shall be followed at all times. Council staff are not permitted to obtain telecommunications and internet use data other than as provided for by the Act. Those persons authorised are shown on page 9 of the guidance.

Authorising Officer

13. All requests for authorisation of directed surveillance or a CHIS under RIPA must be approved in advance by an Authorising Officer. An Authorising Officer is a person who has been delegated power to act in that capacity by the Head of Democratic & Legal Services or relevant Corporate Director with regulatory responsibilities. A list of officers who have, to date, been authorised, is annexed to this policy and is subject to regular review and updating by the Head of Democratic & Legal Services.
14. In order to be approved as an Authorising Officer, that person must have attended a relevant training course on the practical application of RIPA.

Authorisation Process

15. All requests to conduct, renew, review or cancel a covert surveillance exercise or use of a CHIS must be made in advance in writing on the appropriate forms. Please see the forms on the Council's intranet. All such requests must be submitted to an Authorising Officer of the Council.
16. The power to grant, renew, review and cancel will be limited to Authorising Officers in order to ensure greater independence and consistency. Written authorisation for a directed covert surveillance operation will be valid for a maximum of 3 months and for a CHIS a maximum of 12 months, both from the date of the original authorisation or renewal.
17. When completing the forms, a full and detailed description of the operation should be provided. This should specify any equipment to be used as well as maps or sketches to show observation points and target premises. Officers need to take particular care to ensure there are no ambiguities in the description of the operation.
18. Authorisation will only be granted where the action is necessary and proportionate.
19. RIPA first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds for directed surveillance or a CHIS; sections 28(3) or 29(3) of RIPA, respectively.
20. Then, if the directed surveillance or use of the CHIS is necessary, the person granting the authorisation must believe that the directed surveillance or use of a CHIS is proportionate to what is sought to be achieved by the conduct and / or use of that CHIS. This involves balancing the intrusiveness of the surveillance or use of the CHIS on the target and others who might be affected by it against the need for the surveillance or CHIS to be used in operational terms. The use of

surveillance or a CHIS 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 other less intrusive means. The use of surveillance or a CHIS should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

21. Proportionality must be carefully explained, not merely assented. Similarly, merely describing parts of the operation itself is not germane to proportionality. A good explanation of proportionality should refer to three elements:
 - (a) balance the extent of the problem against the size and scope of the operation, demonstrating that it is not a 'sledgehammer to crack a nut',
 - (b) explain that intrusion is to be kept to a minimum
 - (c) show that having considered all other practical courses there is no other way in which the necessary evidence can be obtained i.e. a cover operation is the last resort.
22. The Authorising Officer must state their reasons for believing that the authorisation, renewal or cancellation is necessary. If they do not consider authorisation, renewal or cancellation to be appropriate they must also state their reasons for this on the relevant form.
23. The Authorising Officer's statement should not be a mere rubber stamp. It should include a full account of what is being authorised (the five W's test of Who, What, Why, Where & When) and how and why the Authorising Officer is satisfied that the operation is necessary and proportionate. The Authorising Officer should not be put off by repetition as if challenged in court, the Authorising Officer may be required to demonstrate his own thought process at the time and will be in a weak position if he has to rely upon the applicant's account by adoption.

Collateral Intrusion

24. Before authorising the use or conduct of a source, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.
25. An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this

into account, when considering the proportionality of the use and conduct of a source.

Practical Considerations

26. The Council's requirements for covert surveillance will normally be carefully planned so that the necessary consultations regarding risk assessment, insurance and health and safety can be carried out and the required provisions put in place before surveillance commences. In the event of covert surveillance needing to be carried out in an emergency, authorisation is still required. Where it is not possible for the requesting officer to complete the form, the Authorising Officer must still be consulted. In such an emergency situation, provision is made for oral authorisation to be granted for a maximum of 72 hours. As soon as possible following the Oral Authorisation the written application for authorisation must be completed.
27. General observation forms part of the duties of many enforcement officers and is not usually regulated by RIPA. For example, community wardens may be on patrol to observe or prevent crime. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.
28. Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by its very nature, could not have been foreseen. For example, a community warden would not require an authorisation to conceal him or herself and observe a suspicious person that s/he came across in the course of a patrol. If later, however, a specific investigation or operation is to follow an unforeseen response, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert surveillance / use of a CHIS be given backdated authorisation after it has commenced.
29. Embarking upon covert surveillance or the use of a CHIS without authorisation or conducting surveillance outside the scope of the authorisation will not only mean that the protection afforded by RIPA is negated but may also result in disciplinary action being taken against the Officer / Officers involved.
30. Although, the provisions of RIPA do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for directed surveillance will be necessary.
31. Material obtained through covert surveillance may be used as evidence in criminal proceedings. The proper authorisation of surveillance should

ensure the admissibility of such evidence under the common law, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998. Furthermore, the product of the surveillance described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996.

32. Whilst acknowledging that covert surveillance / use of a CHIS is a last resort, RIPA does afford potential protection against claims of unlawful action. Officers must seek the view of an Authorising Officer if they are in any doubt as to whether RIPA is likely to apply to their investigation or action.
33. Where the use of a CHIS is deployed, a "Handler", who can be an officer of the Council, should be designated to have day to day responsibility for dealing with the CHIS. This will include their security, safety and welfare.
34. The only circumstances where authorisation may be given under this regime is where the investigation is for the purpose of preventing or detecting crime or for preventing disorder.

Special Circumstances

35. The use of vulnerable people / juveniles for a CHIS should only occur in exceptional circumstances and due regard must be had to the Code of Practice.
36. Likewise, if covert surveillance is likely to obtain communications subject to legal privilege, or involve confidential personal or journalistic information or material, the officer should refer to the Code of Practice. An authorisation will then only be merited in exceptional or compelling circumstances.
37. Where Special Circumstances apply officers must obtain authorisation for the action from either the Chief Executive, the relevant Corporate Director of Service, the Head of Democratic & Legal Services or the Head of Policy & Review.

Partnership Working

38. If conducting a relevant RIPA investigation in partnership with, under the direct guidance or supervision of or under a request from another body, officers must first seek the approval of an Authorising Officer.

Training

39. All officers with an enforcement or investigatory function will receive training on the provisions of RIPA.

Central Record of all authorisations

40. Each Authorising Officer will be responsible for maintaining a record of all authorisations, renewals, reviews and cancellations issued by them.
41. The Authorising Officer will also be responsible for forwarding a copy of each and every form completed for that purpose to the Head of Democratic & Legal Services within one week of completing that form. The form should be sent in an envelope marked Private and Confidential and for the attention only of the Head of Democratic & Legal Services. The Head of Democratic & Legal Services will then maintain a Central Record of Authorisations.
42. These records will be retained for a period of at least three years from the ending of the authorisation and should contain the following information:
 - the type of authorisation;
 - the date the authorisation was given;
 - name and rank/grade of the authorising officer;
 - the unique reference number (URN) of the investigation or operation;
 - the title of the investigation or operation, including a brief description and names of subjects, if known;
 - whether the urgency provisions were used, and if so why.
 - if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
 - whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
 - the date the authorisation was cancelled.
43. The Senior Auditor will act as Audit Manager who is responsible for monitoring authorisations and carrying out annual and random reviews of applications, authorisations, reviews, renewals and cancellations.

Conclusion

44. The Head of Democratic & Legal Services, Head of Policy & Review, Senior Auditor and relevant regulatory service heads will review this policy annually.
45. All enquiries about this policy or the applicability of RIPA should be referred at first instance to the Head of Democratic & Legal Services or such other person as they may designate.
46. For additional information / guidance please see the Home Office or Office of the Surveillance Commissioners websites.

Current List of Authorising Officers

Chief Executive

Director of Environmental Services

Director of Community Services

Director of Corporate Services

Head of Policy & Review

Head of Democratic & Legal Services

Head of Environmental Protection

Head of Public Health and Community Development

Head of Planning and Building Control

Chief Finance Officer

Benefits Manager

Single Point of Contact

Head of Policy and Review