

CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000

Introduction

1. The Regulation of Investigatory Powers Act 2000 (**RIPA**) is concerned with the regulation of surveillance and other intelligence gathering by public authorities in the conduct of their legitimate business. These activities are an unavoidable part of modern public life, but only in recent years have they been made the subject of formal statutory control.
2. Section 6 of the Human Rights Act 1998 provides that it is unlawful for a public authority to act in a way which is incompatible with a European Convention right. Article 8 of the European Convention of Human Rights says that everyone has the right to respect for their private and family life, their home and their correspondence.
3. The use of surveillance and other intelligence gathering techniques may amount to an interference with rights protected by Article 8 of the European Convention and could amount to a violation of those rights unless the interference is in accordance with the law.
4. RIPA was enacted to ensure these activities do not infringe the Human Rights Act by establishing a statutory framework which is consistent with the European Convention and by introducing national standards which are applicable to all public authorities.
5. The Council has approved a policy for tackling fraud and corruption. In limited circumstances the Council may wish to use surveillance techniques for the purpose of enforcing this policy or other of its statutory functions. The requirements of RIPA are most likely to apply to those Sections of the Council with enforcement/investigatory functions.
6. RIPA provides a statutory mechanism for authorising covert surveillance and the use of a “covert human intelligence source” (CHIS) e.g. undercover agents. It also permits access to communications data in specific circumstances.

Types of Surveillance

7. Surveillance may be overt or covert.
8. Most of the surveillance carried out by the Council is done overtly – there is nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public, and/or will be going about Council business openly. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisy householder is warned that noise will be recorded if it continues).
9. Surveillance is covert only if it is calculated to ensure that persons who are subject to the surveillance are unaware that it is taking place. RIPA regulates two types of covert surveillance.

10. “Directed surveillance” means covert surveillance that is undertaken:
- in connection with a specific investigation or operation
 - which 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)

‘Private information’ means information relating to a person’s private and family life, their home and their correspondence.

11. Directed surveillance does not include information gathered 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 the surveillance. Directed surveillance may, in the case of a local Authority, only be carried out for the purposes of “preventing or detecting crime or of preventing disorder.”

(Note: In *C v The Police* – 14th November 2006, the Tribunal held that covert surveillance of employees suspected of non criminal activities did not fall into the definition of directed surveillance because it was not for a “specific investigation or operation.” The tribunal interpreted the latter words as requiring an investigation to be carried out for the specific regulatory functions of a public authority not the general functions such as staffing.)

12. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will usually result in the obtaining of private information about that person as well as others that he or she comes into contact or associates with.
13. An example of directed surveillance would be when officers follow a person over a period to find out whether they are working at the same time as claiming benefit. Similarly, although town centre CCTV cameras will not normally require authorisation, if a camera is directed in such a way as to observe a particular individual, authorisation may be required.
14. “Intrusive surveillance” means covert surveillance conducted by means of a person or device located inside residential premises or a private vehicle. A local authority cannot carry out intrusive surveillance.

Conduct and Use of Covert Human Intelligence Resource (CHIS)

15. A person is a **CHIS** if he or she establishes a relationship with another person in order to covertly obtain or disclose information. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic responsibilities or where contact numbers are set up to receive information. Similarly, people who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS because they are not being required to establish or maintain a relationship for a covert purpose.
16. The conduct or use of a CHIS requires prior authorisation. The use of juvenile sources or vulnerable individuals may only be authorised by the Chief Executive. Again, a CHIS may only be used for the purposes of “preventing or detecting crime or of preventing disorder.”

Communications Data

17. This is data held by telecommunications companies and internet service providers. Examples of communications data that may be acquired with authorisation for a specified operation include:
 - names
 - addresses
 - telephone numbers
 - IP addresses – when a session online started and ended and when an email server was accessed but not the website addresses viewed
 - geographical location of the calling or the called parties.
18. Communications data does not monitor content. The sole grounds for taking action under these provisions is for the purposes of “preventing or detecting crime or of preventing disorder.”
19. There are two powers conferred by RIPA on a local authority to collect communications data. One power permits an authorised person to authorise another person in the same public authority to collect the data. i.e. if a communications service provider is technically unable to collect the data the authorisation permits the local authority to collect the communication data itself. The second power permits the public authority to compel a communications service provider to disclose communications data in its possession.
20. Requests for communication data can only be sent by an officer who is known as a Single Point of Contact (‘SPoC’). The SPoC is an officer who has undertaken the requisite training and passed an examination to achieve proper accreditation. Only then will the Home Office authorise that person to act as a SPoC. The authority utilises the SPoC service provided by the National Anti-Fraud Network (NAFN).

Authorisation Process

21. Requests to undertake directed surveillance, or to use a CHIS or to collect communications data can only be lawfully carried out if properly authorised and in strict accordance with the terms of the authorisation.
22. The Secretary of State specifies by statutory instrument the level of officer who may act as Authorised Officers. In this Council, the Chief Executive and the Director, under the Constitution (Part 3, Sec 7 (3) (iii)) are designated to act as Authorised Officers. The Chief Executive or Monitoring Officer may designate other officers to act as Authorised Officers. Authorisations must not be allowed to lapse. They must be reviewed regularly or cancelled.
23. The steps to be followed for each procedure are shown in the flow charts in Appendix 1.

24. For Directed Surveillance or the use of a CHIS or Communications data, only the approved RIPA forms, available on the Home Office website: (<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/>) may be used. Any other form will be rejected by the Authorised Officer. An applicant officer, or an Authorised Officer, if in doubt about the process to be followed, should always seek the advice of the Head of Legal and Support Services or the Senior Auditor before applying for, or issuing, an authorisation under RIPA.
25. The officer requesting the authorisation will be responsible for ensuring that copies of all forms are forwarded to the Senior Auditor within seven days of issue. As a control measure the Senior Auditor will supply the applicant officer with a referenced copy of the authorisation which they should keep in their department in secure storage. Officers should ensure that material passing between them is sent in such a way that it cannot be read or intercepted by other people.

Considering an Application for Authorisation

26. Before signing a form, the Authorised Officer must have regard to this Policy and Procedure, to any relevant Code of Practice, to any advice from the Head of Legal and Support Services or Senior Auditor and to any other relevant guidance.
27. The Authorised Officer must also satisfy himself/herself that the RIPA authorisation is:
 - **in accordance with the law**;
 - **necessary** in the circumstances of the particular case on the ground of preventing or detecting crime or preventing disorder; and
 - **proportionate** to what it seeks to achieve.
28. In considering whether or not the proposed surveillance is proportionate, the Authorised Officer will need to consider whether there are other more non-intrusive ways of achieving the desired outcome. If there are none, the Authorised Officer will need to consider whether the proposed surveillance is no more than necessary to achieve the objective as the least intrusive method will be considered proportionate by the courts.
29. The Authorised Officer will also need to take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance. This is known as collateral intrusion. Measures must be taken whenever practicable to avoid or minimise, so far as practicable, collateral intrusion.
30. 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. This must address health and safety issues through a risk assessment. He or she must also have regard to any adverse impact on community confidence that may result from the use or conduct of the information obtained.

Urgent Authorisations

31. Urgent authorisations should not be necessary. In exceptional circumstances, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. Urgent authorisations will last for no more than 72 hours.

Central Co-ordination

32. The Chief Executive will be the Senior Responsible Officer for the overall implementation of RIPA. The Head of Legal and Support Services will be responsible for:
 - giving advice and assistance to all staff concerned with the operation of the Act;
 - arranging training for all staff concerned with the operation of the Act;
 - maintaining and keeping up to date this corporate policy and procedure.
 - The Senior Auditor will be responsible for:maintaining a central and up to date record of all authorisations;
 -
 - along with the Head of Legal and Support Services, giving advice and assistance to all staff concerned with the operation of the Act;
 - allocating reference numbers to authorisations;

Working with other Agencies

33. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this Policy and Procedure must be used and the agency given explicit instructions on what it may do and how it may do it.
34. When some other agency (e.g. Police, Customs & Revenue etc.):
 - wish to use the Council's resources (e.g. CCTV surveillance systems) for RIPA purposes, that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes he or she must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Senior Auditor for inclusion on the central register);
 - wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, the officer should normally grant the request unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may need to be sought. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not involved in the RIPA activity of the external agency.

Other Sources of Information

35. The Home Office has issued Codes of Practice on surveillance, CHIS and the collection of communications data. These Codes of Practice supplement this policy and procedure document and should be used as a binding source of reference by all those officers whose task it is to apply the provisions of RIPA and its subordinate legislation.

ASG Revised Dec 2006

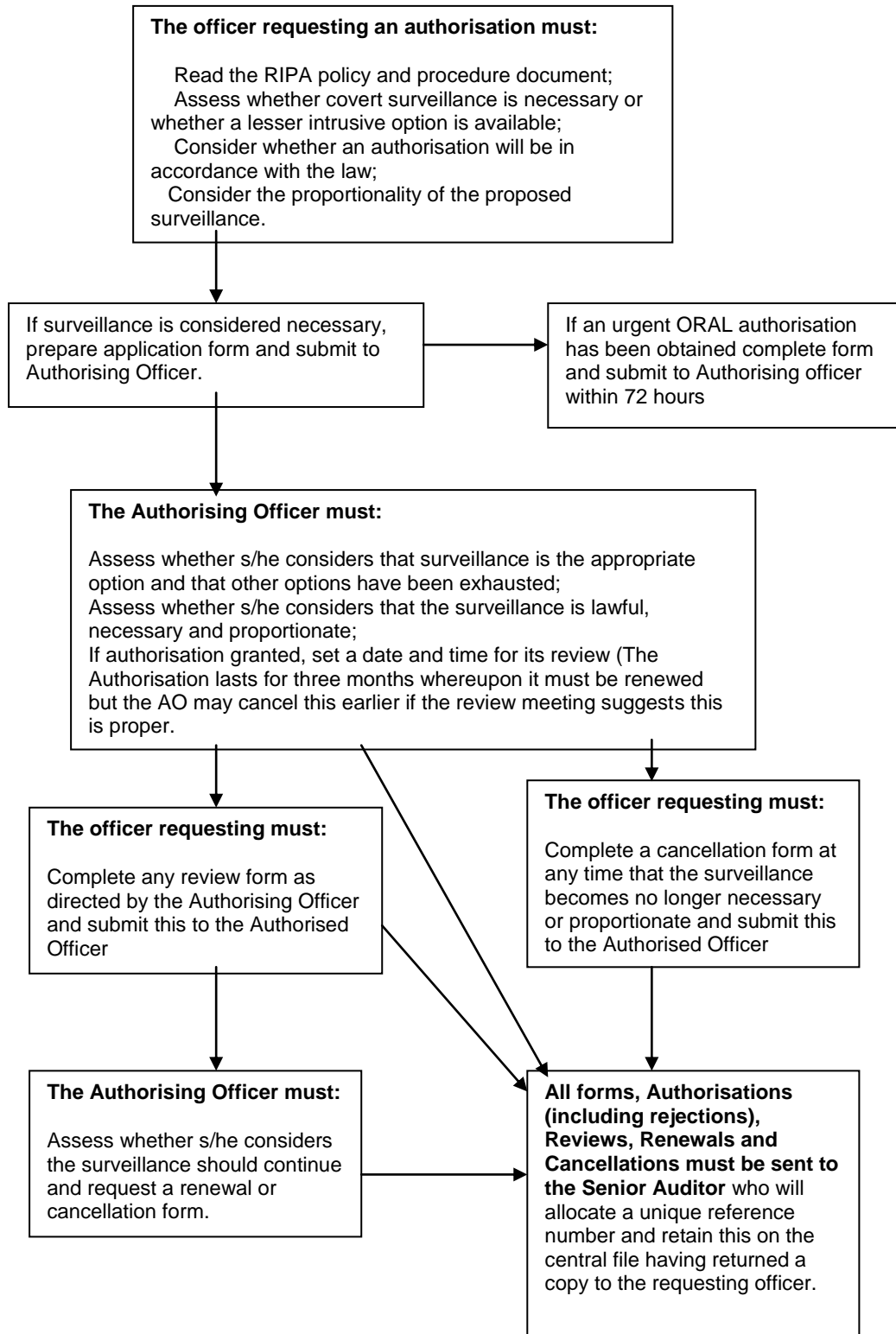
ASG Reviewed May 2009

AW Reviewed and updated June 2010

ASG Revised March 2012

RIPA – DIRECTED SURVEILLANCE / USE OF CHIS PROCEDURE

(Note: Only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS)



Note: There are separate authorisation, review, renewal and cancellation forms for Directed Surveillance and CHIS.

RIPA – COMMUNICATIONS DATA PROCEDURE

