



RIPA 2000



Awarded for excellence

POLICY AND PROCEDURES

TABLE OF CONTENTS

INTRODUCTION

1. DEFINITIONS

- 1.1 Surveillance
- 1.2 Directed covert surveillance
- 1.3 Intrusive covert surveillance
- 1.4 Covert human intelligence source
- 1.5 Accessing communications data

2. LAWFUL PURPOSES FOR UNDERTAKING COVERT SURVEILLANCE

- 2.1 Lawful purposes for directed covert surveillance/use of covert human intelligence sources (CHIS)
- 2.2 Intrusive covert surveillance

3. AUTHORISATION OF COVERT SURVEILLANCE

- 3.1 Authorisation Process
- 3.2 Senior Management role
- 3.3 Management and safety of human intelligence source
- 3.4 Authorisation of human intelligence sources
- 3.5 Authorising officer also acting as controller or handler
- 3.6 Juvenile human intelligence sources
- 3.7 Juvenile sources and information against parents
- 3.8 Time limit on authorisations for directed covert surveillance
- 3.9 Time limit on authorisations for covert surveillance using a CHIS
- 3.10 Time limit on accessing communications data
- 3.11 Review period for authorisations
- 3.12 Urgent oral authorisations
- 3.13 Cancellation of authorisations

4. ACQUISITION OF CONFIDENTIAL MATERIAL

- 4.1 Assessment
- 4.2 Obtaining confidential Material
- 4.3 Definition of confidential material
- 4.4 When information is held in confidence
- 4.5 Seeking advice from legal services on confidential material
- 4.6 Copying and disseminating confidential material
- 4.7 Destruction of confidential material

5. OUTSIDE INTERFERENCE

- 5.1 Consideration of outside interference
- 5.2 Assessment of risk of outside interference
- 5.3 Action if outside interference becomes apparent

6. USING COVERT HUMAN INTELLIGENCE SOURCES

- 6.1 Conditions for use
- 6.2 Record keeping in respect of human intelligence sources
- 6.3 Human intelligence sources and surveillance devices

7. RECORD KEEPING

- 7.1 Holding a central register
- 7.2 Forwarding copy documentation to the Register Holder
- 7.3 Retention of information
- 7.4 Retention for pending or future criminal proceedings
- 7.5 Retention of confidential material
- 7.6 Unrelated material
- 7.7 Subject access under the Data Protection Act 1998
- 7.8 Records in respect of human intelligence sources

8. FUNCTIONS OF THE SURVEILLANCE COMMISSIONER

9. COMPLAINTS AND THE TRIBUNAL

POLICY AND PROCEDURE – DIRECTED SURVEILLANCE, COVERT HUMAN INTELLIGENCE SOURCES AND ACCESSING COMMUNICATIONS DATA

INTRODUCTION

The Regulation of Investigatory Powers Act received Royal Assent on the 28 July 2000 and can be viewed at <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm>

The intention of the Act is to ensure that the relevant investigatory powers are used in accordance with human rights. The investigatory powers that the Act covers are:

- The interception of communications
- The acquisition of communications data, e.g. billing data
- Intrusive covert surveillance, on residential premises/in private vehicles
- Directed covert surveillance in the course of specific operations/investigations
- The use of covert human intelligence sources, e.g. agents, informants, undercover officers
- Access to encrypted data

The policy and procedures that follow do not cover all aspects of the Act, but focus on the main areas that are likely to have an impact on the Service, i.e.

- Directed covert surveillance
- The use of covert human intelligence sources
- Accessing communications data

The Act introduces:

- Lawful purposes for which the investigatory powers can be used, i.e. They cannot be used unless one of these purposes are met.¹
- Formal authorisation of the use of any of the investigatory powers, Which is auditable by Surveillance Commissioners
- Independent judicial oversight
- The means of redress for individuals

This policy and procedure document compliments the Home Office Codes of Practice on covert surveillance, the use of covert human intelligence sources and accessing communications data. All officers involved in covert surveillance operations/investigations should familiarise themselves with the content of these Codes of Practice.

1. DEFINITIONS

1.1 Surveillance

Surveillance Includes:

- Monitoring, observation or listening to persons, their movements, their conversations or other activities or communications;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by, or with assistance of a surveillance device

1.2 Directed Covert Surveillance

- Is for a specific investigation, and
- Is undertaken in a manner where it is likely to result in obtaining private information about an individual (whether or not this is an individual that has been specifically identified for the purposes of the investigation), and
- Is carried out in a manner calculated to ensure that the individuals subject to the surveillance are unaware that it is or may be taking place

Notes:

- Private information about an individual means any information relating to his/her private or family life
- 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 have been foreseen, e.g. an investigating officer may observe a person committing a breach of Service operating policies. The officer would not require authorisation to follow this individual and establish their identity and any other information that may help with subsequent investigation
- Low-level covert activity, which does not involve the systematic surveillance of an individual will also not usually be regulated under the provisions of RIPA, e.g. Fire Safety Officers may covertly observe and then visit a night club as part of their enforcement activities to verify numbers of customers present within the premises which may be liable to restrictions to comply with fire safety regulations. Such observations may involve the use of equipment to re-enforce normal sensory perception, like binoculars or cameras, but it clearly does not involve the systematic surveillance of an individual.

1.3 Intrusive covert surveillance

- Is carried out in relation to anything taking place on any residential premises, or in any private vehicle, and
- Involves the presence of an individual, e.g. an investigating officer, on the premises or in the vehicle, or is carried out by means of a surveillance device, and
- Is carried out in a manner calculated to ensure that the individuals subject to the surveillance are unaware that it is or may be taking place

Notes:

- Residential premises means any premises being occupied or used by an individual, however temporarily, for residential purposes or living accommodation; this includes hotels and guest houses
- Surveillance device means any apparatus designed or adapted for use in surveillance
- If the surveillance device is not present on the premises, or in/on/under/attached to the vehicle then the surveillance will only be classified as intrusive if the device is capable of consistently providing the same quality and detail as if it were. If it is not then the operation or investigation will fall within the definition of directed covert surveillance
- If the surveillance device has been primarily designed or adapted for the purpose of providing information about the location of a vehicle (tracking) then the surveillance will not be classified as intrusive. The operation or investigation will fall within the definition of directed covert surveillance

1.4 Covert Human Intelligence Source

- He/she establishes or maintains a relationship with a person or persons, and
- Covertly uses the relationship(s) to obtain information, or to provide access to information for any other person, or
- Covertly discloses information obtained through the relationship(s), and
- Other parties involved in the relationship(s) that is/are established or maintained are unaware of the purpose of the relationship(s) and/or the intention to use/disclose information acquired as a result of it

Notes:

- There is no geographical limitation on the use or conduct of a source. Authorisations can be granted for the use or conduct of a source both inside and outside the UK
- The use of covert human intelligence sources by the Wiltshire Fire & Rescue Service is likely to be exceptional. This type of activity relates more obviously to the Police and other law enforcement agencies, where informants are often cultivated and then used, i.e. asked, induced or assisted, to engage in specific covert investigations/operations
- Such activity may apply to the Service if officers are asked to work in an undercover capacity, e.g. detached to other Service premises in a new role in order to investigate the loss/misuse of Service equipment
- Any such covert activity must be approached by the Service with caution. By their very nature covert investigations using human intelligence sources are likely to be intrusive and involve outside intrusion or interference and the acquisition of confidential material

1.5 Accessing Communications Data

- This covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself, contents of e-mails or interactions with websites. The word "data" in relation to postal terms means anything written on the outside of the item.

2. LAWFUL PURPOSES FOR UNDERTAKING COVERT SURVEILLANCE

2.1 Lawful purposes for directed covert surveillance/use of covert human intelligence sources and accessing communications data.

- In the interests of national security (unlikely to apply to the Service)
- For the purpose of preventing or detecting crime, or of preventing disorder¹
- In the interests of the economic well being of the UK
- In the interests of public safety²
- For the purpose of protecting public health
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department
- For the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.³

2.2 Intrusive covert surveillance

There are **no circumstances** under which it would be lawful for the Wiltshire Fire & Rescue Service to undertake such operations or investigations.

3. AUTHORISATION OF COVERT SURVEILLANCE

3.1 Authorisation Process

There is a requirement under RIPA 2000 for all covert surveillance investigations that the Wiltshire Fire & Rescue Service is **lawfully empowered to undertake** to be properly recorded and authorised. Such authorisations must be:

- In writing (see para. 3.5 for urgent cases), and
- Approved by a designated senior officer. This person is known as the Authorising Officer. The Service should ensure that they identify Authorising Officers for RIPA purposes. This should **preferably be an officer who does not have an immediate supervision of the officers carrying out the investigation.**
- Any surveillance investigation that has not been properly authorised will be **deemed unlawful** and could lead to a challenge against the whole case under Article 8 of the Human Rights Act.
- Applications for communications data may only be made by persons in the same public authority as a designated person.
- Where appropriate authorisations for communications data should be channelled through a single point of contact (SPOC). This will provide for an efficient regime since the SPOC will deal directly with the postal or telecommunications operator on a regular basis. The SPOC will also advise the designated person on whether an authorisation or a notice is appropriate.

3.2 Authorising Officer Role

The Authorising Officer must satisfy himself/herself that the investigation:

- Meets one of the lawful purposes (see 2.1)
- Is proportionate to what is being sought to be achieved by undertaking it, i.e., that all other options to achieve the desired outcome have been tried or considered,

that covert surveillance is the last resort option and that a sledgehammer is not used to crack a nut. Violation of Article 8 of the Human

- Rights Act may result if investigations are carried out without due regard to an individual's right to privacy
- Is time limited, with a review date arranged

3.3 Management and safety of a human intelligence (“Source”)

Where the use of a Source is being considered, the Authorising Officer should make an assessment of any risk to the Source in carrying out the conduct in the authorisation and the likely consequence should the role of the Source become known to the target. The Authorising Officer should be satisfied that adequate arrangements exist for the management of the Source and that there is at all times a person with responsibility for maintaining a record of the use made of the Source by a (“Controller”). The ongoing security and welfare of the Source after the cancellation of the authorisation should be considered at the outset.

3.4 Authorisation of Sources

Authorisation for the use and conduct of a Source is required prior to asking them to act. If the nature of the task changes a new authorisation may need to be obtained

3.5 Authorising Officer also acting as Controller or (“Handler”)

An Authorising Officer may act as the Controller or Handler of a Source, but **must not** authorise his/her own activities where he/she acts as the covert human intelligence source.

3.6 Juvenile human intelligence sources

Authorisations for the use or conduct of juvenile Sources (those under 18) should not be granted unless:

- A risk assessment has been undertaken as part of the application to deploy the juvenile Source covering the physical dangers and the psychological aspects of his/her deployment
- The Authorising Officer has considered the risk assessment and he/she is satisfied that any risks included in it have been properly explained.
- The Authorising Officer believes that arrangements exist that will ensure that there will be at all times a person who has responsibility for ensuring that an appropriate adult will be present for any meetings between a Source under 16 years of age.

3.7 Juvenile Sources and information against parents

On no occasion should the use of a Source under 16 years of age be authorised to give information against his/her parents.

3.8 Time limit on authorisations for directed covert surveillance

The time limit for authorisation for directed covert surveillance investigations is **three (3) months**. At this stage the case must be reviewed and formally renewed if the Authorising Officer believes that the appropriate criteria, i.e. lawful purpose(s), are still being met.

3.9 Time limit on authorisations for covert surveillance using Sources

The time limit for authorisation for covert surveillance investigations using Sources is twelve (12) months. At this stage the case must be reviewed and formally renewed if the Authorising Officer believes that there are adequate grounds to continue with the investigation.

3.10 Time limit on authorisations and notices for accessing communications data.

Authorisations and notices will be valid for one month. A designated person should specify a shorter period if that is satisfied by the request, since this may go to the proportionality requirements. For future communications data disclosure may only be required of data obtained by the operator within this period up to one month. For historical communications data disclosure may only be required of data in the possession of the postal or telecommunications operator. A Section 22(4) notice under RIPA should be complied with as soon as reasonably practicable to do so. An authorisation or notice may be renewed at any time during the month it is valid.

3.11 Review period for authorisations

Whilst review periods are effectively set by the legislation Authorising Officers should, as a matter of good practice, arrange for **regular reports (at least monthly)** on the progress of covert surveillance investigations.

3.12 Urgent oral authorisation

Authorising Officers may give their authorisation **orally**. Such oral authorisations are only valid for a **seventy two (72) hour period** and must then either be cancelled or confirmed in writing using the appropriate form. A statement that the Authorising Officer has expressly authorised the action should be recorded in writing as soon as reasonably practicable. This should be done by the person to whom the Authorising Officer spoke and later should ideally be endorsed by the Authorising Officer.

An application for communications data may only be made and approved orally, on an urgent basis, where it is necessary to obtain communications data for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

3.13 Cancellation of authorisations

Covert surveillance investigations should be formally ceased or cancelled and such action must be recorded.

4 ACQUISITION OF CONFIDENTIAL MATERIAL

4.1 Assessment

Any application for an authorisation, which is likely to result in the acquisition of confidential material, should **include an assessment** of how likely it is that such material will be required.

4.2 Obtaining confidential material

Applications for authorisations where it is likely that a substantial proportion of the material obtained could be confidential (see 4.3 for definition) should be subject to rigorous scrutiny and **only approved in exceptional circumstances, with full regard to the 'proportionality test'**.

4.3 Definition of confidential material

'Confidential material' is defined as information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

- To his/her physical or mental health; or
- To spiritual counselling or other assistance given or to be given, and which a person has acquired or created in the course of any trade, business, profession or other occupation, for the purposes of any paid or unpaid office. It includes **both oral and written** information and also communications as a result of which personal information is acquired or created.

4.4 When information is held in confidence

Information is held in confidence if:

- It is held subject to an express or implied undertaking to hold it in confidence; or
- It is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

4.5 Seeking advice from legal services on confidential material

Where any material is acquired as a result of an investigation those handling the material should be alert to anything, which may fall within the definition of confidential material. Where there is doubt as to whether material obtained through covert surveillance is confidential advice should be sought from the Service Solicitor before such material is disseminated.

Confidential material should not be retained or copied unless it is necessary for a specified purpose.

4.6 Copying and disseminating confidential material

The retention or dissemination of confidential information should be accompanied by a clear warning of its confidential nature. Taking reasonable steps to ensure that there is no possibility of it becoming available, or its contents being known to any person whose possession of it might prejudice any criminal or civil proceedings relating to the information should safeguard it.

4.7 Destruction of confidential material

Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

5 OUTSIDE INTERFERENCE/INTRUSION

5.1 Consideration of outside interference/intrusion

Particular consideration should be given to outside interference or intrusion into the privacy of persons other than the subject(s) of surveillance. Such interference or intrusion would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

5.2 Assessment of risk of outside interference/intrusion

Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the investigation. An application for an authorisation

should **include an assessment** of the risk of any outside interference or intrusion. The Authorising Officer must take this into account, particularly when considering the **proportionality of the surveillance**.

5.3 Action if outside interference or intrusion becomes apparent

Those carrying out the covert surveillance should inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation 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.

6 USING COVERT SOURCES

6.1 Conditions for use

There are a number of conditions that RIPA applies if a covert Source is to be used as part of an investigation. These are:

- An officer of sufficient seniority must take day-to-day responsibility for dealing with the individual operating as the human intelligence source who is to ensure the Sources security and welfare. This person is known as a "Handler."
- Another, **different officer** of sufficient seniority must assume responsibility for the general oversight and use made of the individual operating as the human intelligence source. This person is known as a "Controller."
- The Handler is responsible for bringing to the Controller's attention any concerns about the personal circumstances of the Source affecting the risk assessment, the conduct of the investigation and the safety and welfare of the Source. If appropriate the Controller must ensure that the Authorising Officer considers any concerns and a decision is taken on whether or not to allow the authorisation to continue.
- The Controller must **maintain a record** of the **use** made of the individual operating as the Source.

6.2 Record keeping in respect of Sources

There are a number of considerations in maintaining records in respect of an investigation utilising a Source, these are:

- The records maintained about a Source should maintain the confidentiality of the Source and the information provided by that Source.
- The records should contain any significant information provided by that Source.
- The records should contain any significant information connected with the security and welfare of the Source.
- Any risks to the security and welfare of the Source should be properly explained to and understood by the Source.
- Records that disclose the identity of the Source must not be made available to anyone unless there is need for access to be made available to those persons.

6.3 Sources and surveillance devices

A Source wearing or carrying a surveillance device and invited into residential premises or a private vehicle does not require special authorisation to record activity taking place inside those premises or vehicle. The equipment may not be used, however, other than in the presence of the Source, otherwise this would amount to intrusive covert surveillance.

7. RECORD KEEPING

7.1 Holding a central register

The Data Information Security Officer will hold a central register of authorisations. This register will contain the minimum amount of information to meet the requirements of the Surveillance and Communications Commissioners. Register information will be held for 5 years from the date that the authorisation was cancelled or ceased.

7.2 Forwarding copy documentation to the register holder

A copy of the completed authorisation, renewal and cancellation forms must be forwarded to the Data Information Security Officer in order for the central register to be maintained. Copies will be destroyed once register details have been entered.

7.3 Retention of information

The Data Information Security Officer should retain detailed authorisation and other documentation relating to a covert surveillance investigation for at least 5 years from the date that the authorisation was cancelled or ceased. This information is confidential and should be available on a 'need to know' only basis.

7.4 Retention for pending or future disciplinary proceedings

If it is likely that the records could be relevant for future or pending disciplinary proceedings they may be retained for a longer period, always provided that it can be adequately demonstrated that they are still relevant to the purpose for which they were obtained. The senior authorising officer should determine the extended retention period.

7.5 Retention of confidential material

Information of a confidential nature (see para 4.3 and 4.7) should be destroyed as soon as it is no longer relevant to the specified purpose.

7.6 Unrelated material

Where material is obtained by surveillance, which is wholly unrelated to a disciplinary or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or disciplinary proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of Authorising Officer.

7.7 Subject access under the Data Protection Act 1998

Authorising Officers should bear in mind the access rights of individuals to their personal information under the Data Protection Act 1998 and the access rights that will be afforded under the Freedom of Information Act 2000 which will be implemented in Feb 2005.

7.8 Records in respect of Sources

Records in respect of Sources should be maintained in such a way as to preserve the confidentiality of the Source. The Code of Practice issued by the Home Office requires the records to contain a number of particulars and reference should be made to this document for further details. The main items are:

- The security of the Source
- Security and welfare arrangements
- The identity of the Handler and Controller
- The tasks assigned to the Source
- Contacts between the Source and the Handler
- The information received
- The authorisation
- The renewal or cancellation of an authorisation and the reasons why

8. FUNCTIONS OF THE SURVEILLANCE COMMISSIONERS

The Act provides for a Surveillance Commissioner and a Communications Commissioner whose roles are to provide independent oversight of the use of the powers contained within the Act.

The Wiltshire Fire & Rescue Service is under a duty to comply with any request made by the Commissioners and to provide any information they may require when reviewing the operation of the Act by the Service.

9. COMPLAINTS AND THE TRIBUNAL

The Act establishes an independent Tribunal as a means of redress for those who wish to complain about the use of investigatory powers under the Act.

It has full powers to investigate and decide any case within its jurisdiction. It has power to award compensation, quash or cancel any authorisations and require the destruction of records of information.

The complaints process is explained in more detail in leaflets published by the Investigatory Powers Tribunal entitled; 'Information Leaflet' and 'Human Rights Claim Form – T1'. These are available on application to:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1 9ZQ