# Regulation of Investigatory Powers Act 2000

## Executive Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') sets out the procedures that must be followed before making use of:

- covert, directed surveillance techniques;
- covert human intelligence sources; or
- accessing communications data

HWFRS has no record of using the covert techniques covered by RIPA and it is not envisaged we will need to do so in future but we are nonetheless required to have a policy in place to deal with that eventuality should it arise.

Applications to use the covert techniques covered by RIPA must be made using the appropriate Home Office forms and must be approved by one of the designated 'Authorised Officers' set out in this policy.

## Contents

# Regulation of Investigatory Powers Act 2000

## 1. INTRODUCTION

1.1. The Human Rights Act (HRA) 1998 was introduced to give effect to the European Convention on Human Rights (ECHR) and came into force in October 2000. The HRA imposes a duty upon public authorities, including Hereford and Worcester Fire and Rescue Service (HWFRS), to act in ways that are compatible with the rights under the ECHR. Failure to do so may enable a person to seek damages against the Service or to use our failure as a defence in any proceedings that we may bring against them.

1.2. The Regulation of Investigatory Powers Act 2000 ("RIPA") sets out procedural rules to enable specified public authorities to use covert investigatory techniques which might otherwise infringe legal rights to privacy and respect for family life under the HRA. In particular they govern when and how hidden surveillance, covert witnesses and interception of communications can be used. HWFRS is included in the list of public authorities which can rely on RIPA.

1.3. HWFRS has no history of using the covert investigatory techniques covered by RIPA and there is no expectation that there will be a need to use them in the future. It is anticipated that HWFRS will usually be able to gather all the information required for its statutory functions without covert information gathering. This policy does not change this position. The purpose of this policy is to:

(a) reinforce advice to officers that the use of covert investigatory techniques should be avoided in most circumstances; and

(b) ensure that should the unforeseen and exceptional eventuality arise when reliance on RIPA is needed there will be a clear procedure for handling its use.

1.4. The protection of RIPA is available to HWFRS only when carrying out its core functions as a fire and rescue authority. RIPA does not apply to the ordinary general functions carried out by all authorities e.g. staff disciplinary or contractual issues. Another legal basis for avoiding infringing rights to privacy would be needed in these circumstances.

1.5. This policy is intended to ensure that HWFRS policy and practice are in line with the Codes of Practice and guidance issued under RIPA. In any proposed utilisation of RIPA powers, reference should be made to the Codes of Practice and guidance published on the Home Office website and by the Office of Surveillance Commissioners http://surveillancecommissioners.independent.gov.uk/.

## 2. ACTIVITIES COVERED BY RIPA

2.1. There are three forms of covert intelligence gathering that are covered by RIPA and potentially available to HWFRS: Directed Surveillance; Covert Human Intelligence Sources and Accessing Communications Data.

2.2. **Directed surveillance** is:

- **Surveillance** (i.e. monitoring, observing or listening to people or their movements, conversations or other activities)
- **which is covert** (i.e. done in a manner calculated to ensure that the subject is unaware that it is taking place)
- **that is carried out in relation to a specific investigation or operation** (i.e. not as routine observations of people or an area in general)
- and which is **likely to result in obtaining private information** about any person (i.e. any information about a person's private or family life including names, phone numbers or even business relationships).

a) It does **not** include circumstances where this is done by way of an immediate response to events (as it would not be practicable for that to have prior authorisation).

b) Any covert surveillance of what takes place in residential premises or a private vehicle is deemed as "intrusive" and outside what HWFRS may lawfully do even under RIPA.

c) Overt and sign-posted use of CCTV cameras (on premises or on vehicles) is not Directed Surveillance because it is neither covert nor carried out in relation to a specific investigation or operation. C*overt* use of hidden CCTV cameras may be Directed Surveillance but only if this were part of a specific investigation or operation rather than the usual placing of cameras for general surveillance.

2.3. **Covert Human Intelligence Sources**

A Covert Human Intelligence Source (CHIS) is somebody who:

- **establishes or maintains a personal or other relationship with a person:**
- EITHER **for the covert purpose of obtaining information** (i.e. any information whether private or not)
- OR for the purpose of **covertly disclosing information obtained by the use of such a relationship**

a) "Covert" means in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use of the relationship or disclosure of information.

b) A CHIS must also necessarily have a relationship with another party. So a stranger to the subject who has been asked to "keep an eye" on comings and goings from particular premises would not be a CHIS as they have no relationship that provides the information (but they might need to be authorised for Directed Surveillance).

c) The need for a CHIS authorisation is not limited to cases where someone has been tasked with obtaining information. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. A member of the public who voluntarily provides information obtained by covert means on a regular basis would be a CHIS. The Authority would owe that person a duty of care and must consider whether using the information provided might place the informant at risk.

d) No CHIS authorisation is needed where there is another legal basis for a person to report information covertly (e.g. a professional duty to comply with regulations).

e) Any type of relationship could be covered, e.g. a customer of a business. However statutory guidance suggests that a simple "one-off" transaction may not be sufficient interaction to constitute a "relationship", and that more extensive engagement between the two parties would be needed, e.g. for the CHIS to be a regular buyer of "under the counter" goods from a certain supplier

2.4. **Accessing Communications Data**

A third technique of covert investigation is currently open to the Authority under RIPA: accessing communications data. Postal or telecommunications service providers hold certain types of communications data. RIPA gives fire authorities (along with other local authorities) a power to access this data. The communications data that can be obtained by fire authorities is strictly limited and extends only to:

(a) **Subscriber information** – i.e. information about the customer's account: name of the customer who is the subscriber for a telephone number/ e-mail account etc.; account information such as address for billing, delivery or installation; details of payments and bank or credit/ debit card details; Information provided by the subscriber to the Communications Service Provider such as demographic information or sign up data (other than passwords) such as contact telephone numbers; ***AND***

(b) **Service Use Data** – i.e. the general ways in which the service was used: periods during which the customer used the service; itemised records of telephone numbers called, Internet connections, dates and times of calls, duration of calls, text messages sent and quantities of data uploaded or downloaded; records of postal items, such as records of registered, recorded or special delivery postal items and records of parcel consignment, delivery and collection.

2.5. Fire Authorities (like local authorities generally) are NOT empowered to obtain what is called "**traffic data**" which is specific information about communications i.e. what websites visited, the origins of incoming calls, mobile phone cell site locations. The Authority could not access the *content* of an individual's communications.

## 3. WHEN RIPA PROCEDURES CAN BE USED

3.1. The covert intelligence gathering techniques under RIPA can be used only in certain prescribed circumstances. These are where:

(a) their use is **necessary** for:
- the prevention or detection of crime;
- preventing disorder; or
- in the interests of public safety or the protection of public health;

**and**

(b) their use is **proportionate** to the purpose of the operation.

(For **Accessing Communications Data** part (a) is limited to the prevention or detection of crime or preventing disorder or in the interests of public safety.)

3.2. Also, RIPA can be relied on only where it is exercised in accordance with **due process**. This means that the procedure in this policy must be followed and the Authority must abide by the relevant Code of Practice issued by the Home Office and published on the Home Office website.

3.3. RIPA can be relied on only in carrying out HWFRS' specific functions as a fire and rescue authority e.g. it is potentially available to help in statutory fire safety work. However, RIPA would not be available for "ordinary" functions common to any public authority such as employing staff or contracting with a supplier of goods or services.

3.4. In deciding whether the "necessary and proportionate" test is passed officers must consider whether the proposed activity is an appropriate use of the legislation and a reasonable way of obtaining the necessary result. In particular this must include consideration of:

(a) Whether information could be gathered by **alternative overt means** e.g. evidence of non-compliance with fire regulations might be obtained from a well-timed unannounced visit to inspect rather than by covert surveillance;

(b) The **size and scope of the proposed activity** against the gravity and extent of the possible crime (or other harm) being investigated;

(c) How to minimise the impact of any intrusion on the subject or others;

(d) Whether there is a risk of "collateral intrusion" i.e. whether there will be any interference with the privacy of a third party who is not the subject of the covert activity. This might include family members, customers or other associates of the subject. Where there is such a risk it should be considered whether that interference is itself necessary and proportionate and whether the risk can be mitigated;

(e) Whether there is a risk of confidential information being revealed. The Codes of Practice identify confidential personal information, confidential information held for the purposes of journalism, confidential information passing between an MP and a constituent and confidential information concerning spiritual/religious counselling as well as information that is legally privileged i.e. passing between a person and a legal advisor. If there is a risk of revealing information that is legally privileged, specific legal advice is required.

## 4. THE APPROVAL PROCESS

### Approval process for Directed Surveillance and Covert Human Intelligence Sources

4.1. The covert investigation techniques covered by RIPA can only be used with the appropriate approval in place. This approval process is outlined below.

4.2. The first step is for investigating officers to consider for themselves whether the use of a covert investigation technique is necessary and proportionate. A full written record of this preliminary consideration should be made and retained. It is envisaged that this self-assessment will invariably show that covert investigation is avoidable as alternatives are available. If so, the matter ends there.

4.3. If it continues to look like covert surveillance is necessary and proportionate an application for approval should be made only by a Group Commander or equivalent on the appropriate Home Office form, available from their website at http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/. Applications for approval are to be made to the Authority's designated RIPA Authorising Officers:

Chief Fire Officer
Deputy Chief Fire Officer
Assistant Chief Fire Officer

(Only the Chief Fire Officer is authorised to approve the use of CHIS)

4.4. The Authorising Officer will decide whether to approve the use of one of the RIPA techniques and on what terms (if any) they may be used. The Authorising Officer must issue all authorisations in writing. No covert surveillance can begin until this authorisation is issued.

4.5. Any authorisation must be time limited for a set period from the date of the approval as follows:

**Directed Surviellance – 3 months (less one day)**
**CHIS - 12 months (less one day)**

In addition, when granting approval the Authorising Officer must set an appropriate review date (which must not be longer than one month). The Authorising Officer must review the continuing need for the authorisation on the review date – any approval should not last longer than is justified by the "necessary and proportionate" test and an approval will have to be cancelled early if a review shows it is no longer justified. If, on review, an authorisation is allowed to continue in force then a further review date must be set.

4.6. At the expiry of an authorisation it must be formally cancelled by the Authorising Officer and not allowed simply to lapse. Again the appropriate Home Office form is to be used for this. An authorisation may be renewed by a further application to the Authorising Officer on the appropriate form. If so, it will be necessary to show that the tests in this policy continue to be satisfied. In any case the Authorising Officer must continue to ensure appropriate and regular reviews of the authorisation (to be at least monthly).

4.7. Additionally, when authorising a CHIS the Authorising Officer must ensure before granting an authorisation that there is a "handler" in place. This handler will have day-to-day contact with the source and general oversight of them. The handler directs the source's day-to-day activities, records information supplied by the source and monitors the source's welfare and security. Officers seeking a CHIS approval must therefore include in the application an assessment of the personal, operational and ethical risks of using the CHIS, including the likely consequences to the CHIS of the role becoming known. This assessment must be kept with the other records of the approval in accordance with the policy on record keeping in part 5 of this policy. The Authorising Officer will not approve as a CHIS anyone who is:

(a) a vulnerable adult (i.e. a person who may need community care services by reason of mental or other disability, age or illness and may be unable to take care of him/herself or protect him/herself from harm or exploitation); or

(b) under the age of 18.

4.8. Applications for approval may be made orally in cases of genuine emergency where the time required for the full application process would be likely to endanger life or jeopardise the investigation. Nevertheless, as soon as possible a record of the oral application and its approval (or otherwise) must be made. This should clearly state the reasons why the usual written process could not be used.

4.9. There are extensive requirements relating to record keeping when a CHIS is used. These are set out in 5.4 below.

4.10. It should be noted that this RIPA process establishes no more than that the covert operation would be lawful. Officers must ensure that all other appropriate planning and risk assessments (e.g. health and safety) are also in place.

**Approval process for Access to Communications Data**

4.11. Additional steps beyond those in 4.1-10 above are required to approve access to communications data to ensure any information received is handled in accordance with the law.

4.12. Where the Authorising Officer wishes to approve an application to access Communications Data the decision must then be referred to a designated Single Point of Contact ("SPoC") appointed by the Authorising Officer. The SPoC is responsible for facilitating the handover of any data in accordance with the law. The SPoC will review the approval from the Authorising Officer and consider whether:

(a) the application has been properly made in accordance with due process; and

(b) it is reasonable practicable or possible to obtain the communications data requested.

If satisfied of these the SPoC returns the application to the Authorising Officer to make a final approval decision. It is for the SPoC to prepare a Notice in the form prescribed by the Home Office and to serve this on the service provider. The service provider will provide the data to the SPoC who should deliver it direct to the Authorising Officer.

4.13. Anyone who is to act as a SPoC must have attended an accredited course and obtained a PIN reference from the Home Office. The PIN reference is produced to the service provider with any request for data in order to confirm the SPoC is able to receive the data lawfully. In the absence of a member of staff being trained and accredited as a SPoC, the Authorising Officer may appoint an external provider such as the National Anti-Fraud Network (NAFN) to undertake the SPoC service.

4.14. There currently are two approved SPoC officers within HWFRS:

Deputy Chief Fire Officer

Station Commander, Fire Control

4.15. RIPA makes provision for HWFRS to obtain communications data lawfully. The handling and storing of that data will also be governed by the Data Protection Act 1998 so regard must also be had to the Authority's policy on data protection.

## 5. RECORD KEEPING

5.1. In accordance with best practice in the Home Office Codes the Authority has appointed the Head of Legal Services (Clerk & Monitoring Officer) to be its Senior Responsible Person ("SRO"). The SRO is a senior manager with oversight of compliance with RIPA. The SRO therefore has overall responsibility for:

(a) The integrity of the Authority's procedures for managing RIPA;

(b) The Authority's compliance with RIPA and the Codes of Practice;

(c) Dealing with external inspectors as appropriate, including monitoring the implementation of any post-inspection action plans.

5.2. Individual Authorising Officers must:

(i) retain a copy every completed form in respect of each:
- authorisation approved by them
- review
- renewal; and
- cancellation

(ii) pass a copy of each of the above forms to the Head of legal Services who will maintain a central register with unique reference numbering of all requests and authorisations for covert surveillance under RIPA over at least the previous three years. This register must also include applications refused, stating the reasons for any refusal.

5.3. Alongside the register the Authorising Officer must maintain a copy of all completed forms including cancellations and renewals so that details of the applicant, the subject, length of the operation, mitigation measures etc. are all retained.

5.4. For a CHIS, records must be kept in a way that ensures the source and any information provided by the source remains confidential e.g. that no information is made available to officers unless it is necessary for them to see it. The Authorising Office (in this case, the Chief Fire Officer) should ensure an appropriate officer is designated with responsibility to ensure confidentiality. The following must also be recorded (and records retained for at least three years):

(a) the actual identity of the CHIS;

(b) the identity used by the CHIS if any;

(c) any other investigating authority involved, and the means by which that authority identifies the CHIS;

(d) any information significant to the security and welfare of the CHIS;

(e) any confirmation by an Authorising Officer, in this case the CFO, that the relevant information has been considered and any identified risks been properly explained and understood by the CHIS;

(f) when and how the CHIS was recruited;

(g) the identities of the handler and others authorising activities including times and dates when they were authorised;

(h) the tasks given to sources and any demands made by the source in relation to his or her activities;

(i) all contacts and communications between the source and the handler;

(j) any information obtained from the source and any dissemination of it;

(k) any payment, benefit or reward provided to the source.

## 6. OVERSIGHT & REVIEW

6.1 The Head of Legal Services as SRO maintains general oversight of the Authority's use of RIPA and compliance with legal requirements and the Codes of Practice. The Surveillance Commissioners and Interception of Communications Commissioner provide external oversight and from time to time may inspect the Authority's policies and practice in regard to RIPA. The SRO has a duty to ensure the reporting of any errors in the use of RIPA to the relevant Commissioners and to ensure any remedial actions required by the Commissioners are taken.

6.2 In accordance with the codes of practice, the Authority's Policy & Resources Committee will review the policy on the use of RIPA at least annually. The annual report to Members will also detail (in an anonymised form) any use by HWFRS of RIPA. This is to ensure Members are able to judge whether the policy is being applied appropriately. For the avoidance of doubt, elected Members have no role in approving or refusing any particular application to use RIPA procedures.