HUMBERSIDE FIRE AND RESCUE SERVICE

Service Improvement

Regulation of Investigatory Powers Act 2000 (RIPA) Policy

Owner	**Assistant Chief Fire Officer**
Responsible Person	**Head of Corporate Assurance**
Date Written	**September 2026**
Date of Last Review	
Date of next review	**September 2028**
EIA Completed	**September 2026**

CONTENTS

1. Introduction
2. Equality, Diversity and Inclusion
3. Aim and Objectives
4. Associated Documents
5. Definitions
6. General Information on RIPA
7. Surveillance
8. Covert Human Intelligence Source (CHIS)
9. Roles and Responsibilities
10. Authorisation Procedures (CHIS)/ Directed Surveillance
11. Duration of Authorisations
12. Working with/through Other Agencies
13. The Use of Social Media
14. Training
15. Records Management
16. Investigatory Powers Commissioner (IPC)

1. INTRODUCTION

Humberside Fire and Rescue Service (HFRS) is committed to fulfilling its statutory responsibilities under the Regulation of Investigatory Powers Act 2000 (RIPA) and associated Home Office Codes of Practice. The Service will act lawfully, fairly, and proportionately when conducting investigations involving covert surveillance or the use of a Covert Human Intelligence Source (CHIS).

HFRS will ensure that any interference with an individual's right to privacy under Article 8 of the European Convention on Human Rights is necessary, justified, and proportionate to the purpose of the investigation. All authorisations for covert surveillance or CHIS will follow strict procedures, including consideration of collateral intrusion, and will be subject to regular review, renewal, and cancellation as required. This Policy is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA'), Home Office Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources and Home Office Guidance.

While fire and rescue services are not typically engaged in criminal investigations, they may occasionally need to use investigatory powers for:

- **Arson investigations** in collaboration with police.
- **Internal investigations** involving staff misconduct or fraud.
- **Public safety operations** where surveillance may be necessary.

HFRS is included in the list of public authorities that can rely on RIPA to authorise covert directed surveillance or the use of a Covert Human Intelligence Source.

Core Code of Ethics

HFRS has adopted the Core Code of Ethics for Fire and Rescue Services. The Service is committed to the ethical principles of the Code and strives to apply them in all we do; therefore, those principles are reflected in this Policy.

National Guidance

Any National Guidance which has been adopted by HFRS, will be reflected in this Policy.

2. EQUALITY, DIVERSITY AND INCLUSION

HFRS has a legal responsibility under the Equality Act 2010, and a commitment, to ensure it does not discriminate either directly or indirectly in any of its functions and services or in its treatment of staff, in relation to race, sex, disability, sexual orientation, age, pregnancy and maternity, religion and belief, gender reassignment or marriage and civil partnership. It also has a duty to make reasonable adjustments for disabled applicants, employees and service users.

3. AIM AND OBJECTIVES

HFRS takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action when carrying out investigations which involve the use of covert surveillance.

HFRS will, at all times, take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (called 'collateral intrusion'), and consider whether any measures should be taken to avoid or minimise collateral intrusion as far as possible. This document may be amended from time to time as necessary, to ensure compliance with the relevant legislation and will be reviewed bi-annually.

4. ASSOCIATED DOCUMENTS

- Equality Impact Assessment
- Legal References –
    - Regulation of Investigatory Powers Act 2000 (RIPA)
- National Guidance Reference –
    - Covert Surveillance and Property Interference Revised Code of Practice - Home Office
    - Covert Human Intelligence Sources Revised Code of Practice - Home Office

5. DEFINITIONS

Term	Definition
Authorising Officers	Officers designated to consider applications and, where the statutory tests are met, grant, review, renew or cancel authorisations for directed surveillance or the use or conduct of a CHIS. They must be satisfied that the activity is lawful, necessary and proportionate and that collateral intrusion has been properly considered.
Covert Human Intelligence Source (CHIS)	A person who covertly establishes or maintains a personal or other relationship with another person for the covert purpose of obtaining or providing access to information, or covertly discloses information obtained through such a relationship.
Covert Human Intelligence Source (CHIS) Controller	The officer responsible for managing and supervising the CHIS Handler and providing general oversight of the use or conduct of the CHIS, including ensuring appropriate arrangements for tasking, security and welfare.
Covert Human Intelligence Source (CHIS) Handler	The officer with day-to-day responsibility for dealing with a CHIS on behalf of HFRS, directing the CHIS's activities, recording information supplied and monitoring the CHIS's security and welfare.

Term	Definition
Covert Surveillance	Surveillance carried out in a manner calculated to ensure that any person who is subject to it is unaware that it is or may be taking place.
Directed Surveillance	Covert surveillance that is not intrusive surveillance; is undertaken for a specific investigation or operation; is likely to obtain private information about a person; and is not carried out as an immediate response to circumstances in which it would not be reasonably practicable to seek prior authorisation.
Intrusive Surveillance	Covert surveillance relating to anything taking place on residential premises or in a private vehicle that involves an individual being present on the premises or in the vehicle or is carried out using a surveillance device. Statutory exceptions apply, including certain location-tracking devices and devices used from outside the premises or vehicle that do not provide information of equivalent quality and detail.
Overt Surveillance	Surveillance carried out openly, or in circumstances where the person being observed is aware that it is taking place. It does not normally require authorisation under RIPA, although other legal and policy requirements may apply.
RIPA Co-ordinating Officer	The officer who coordinates HFRS's RIPA arrangements, maintains the RIPA Register and associated documentation, checks submissions for completeness, organises training and promotes awareness of RIPA requirements.
Senior Responsible Officer	The senior officer with overall responsibility for ensuring that HFRS complies with RIPA and the relevant Codes of Practice, maintains the integrity of its authorisation processes and addresses any compliance or oversight issues.
Surveillance	Monitoring, observing or listening to persons, their movements, conversations or other activities or communications; recording anything monitored, observed or listened to; or surveillance by or with the assistance of a surveillance device.

6. GENERAL INFORMATION ON RIPA

The Human Rights Act 1998 (which brought much of the European Convention on Human Rights into UK Law) requires HFRS, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and correspondence.

The European Convention did not, however, make this an absolute right. This is a qualified right and accordingly HFRS can, in certain circumstances, interfere in a private citizen's right, if such interference is:

(a) in accordance with the law,
(b) necessary (as defined in this policy), and
(c) proportionate (as defined in this policy).

RIPA provides a statutory mechanism (i.e. 'in accordance with the law') for authorising covert surveillance and the use of a 'Covert Human Intelligence Source' ('CHIS'). It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the Act seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

Directly employed HFRS staff and external agencies working for HFRS are covered by the Act for the time that they are working for HFRS. All external agencies must comply with RIPA and the work carried out by agencies on HFRS' behalf must be properly authorised by one of HFRS' designated Authorising Officers.

7. SURVEILLANCE

Surveillance

'Surveillance' can be overt or covert and includes:

(a) monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications, monitoring social media sites;
(b) recording anything mentioned above in the course of authorised surveillance, and
(c) surveillance, by or with, the assistance of appropriate surveillance device(s).

Overt Surveillance

Most of the surveillance carried out by HFRS will be done overtly - there will be 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 i.e. simply watching something that is emerging in front of them.

Surveillance will be overt if the subject has been informed it will happen.

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place (Section 26(9)(a) of RIPA). RIPA applies to Covert Surveillance.

Intrusive Surveillance

This is when surveillance is covert; relates to residential premises or private vehicles and involves the presence of a person on the premises or in the vehicle or is carried out by a surveillance device placed within the premises/vehicle. Surveillance

equipment mounted outside the premises will not be intrusive unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

This form of surveillance can only be carried out by police or other law enforcement agencies. HFRS staff are referred to the Home Office Code of Practice 'Covert Surveillance and Property Interference'.

Examples of types of surveillance

Overt

(a) CCTV recording on fire appliances;
(b) Police Officer or Park Warden on patrol in Uniform.
(c) Signposted Town Centre CCTV cameras (in normal use).
(d) Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists.

Covert (which requires authorisation)

(a) Officers follow an individual or individuals over a period, to establish whether he is working when claiming benefit.
(b) Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop- owner, e.g. where he is suspected of running his business in an unlawful manner.

Directed surveillance

This form of surveillance is regulated by RIPA and is surveillance which:

(a) is covert; and
(b) undertaken for the purpose of a specific investigation or operation; in
    (i) a manner likely to obtain private information about an individual, whether or not that person is specifically targeted for purposes of an investigation, and
    (ii) is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable.

HFRS can authorise directed surveillance for purposes where:

(a) its use is necessary for:
    - the prevention or detection of crime or of preventing disorder; or
    - in the interests of public safety; and
(b) its use is necessary and proportionate to the purpose of the operation[1]

[1] See Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010/521 in particular schedule 1

HFRS will need to demonstrate that it is necessary to use covert surveillance in the proposed operation.

RIPA can be relied on only in carrying out HFRS' specific functions as a fire and rescue authority e.g. it is 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.

In order to demonstrate the necessity, there must be an identifiable criminal offence, or public safety issue which requires investigating.

The operation must also be proportionate. An application and subsequent authorisation must demonstrate how the activity is proportionate in what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut').

Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is not sufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It is equally unacceptable to consider lack of resources or a potential cost saving as sufficient ground to use technological solutions which are often capable of being more intrusive, rather than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

The following four elements of proportionality need to be fully considered, detailed and explained in any application/authorisation:

(a) the balancing of the size and scope of the operation against the gravity and extent of the perceived mischief, (use maps where necessary),
(b) how and why the methods to be adopted will cause the least possible intrusion on the target and others,
(c) is the activity an appropriate use of the legislation and the only reasonable way, having considered all other options, of obtaining the necessary result, and
(d) what evidence there is and what other methods have been considered and why they were not implemented.

The 'authorisation' to carry out the surveillance lasts for **three months** for Directed Surveillance. However, whether the surveillance is carried out or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, the forms do not expire. The forms have to be reviewed, renewed and/or cancelled (once they are no longer required).

8. COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

A CHIS is someone who establishes or maintains a personal or other relationship for the covert purpose obtaining information. RIPA does not apply in circumstances where members of the public volunteer information to HFRS as part of their normal civic duties, or to contact numbers set up to receive information.

The conduct or use of a CHIS requires prior authorisation.

a) Conduct of a CHIS means establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
b) Use of a CHIS includes actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

HFRS can utilise the services of a CHIS only if RIPA procedures, detailed in this document are followed.

Before a CHIS can be tasked, the Authorising Officer will need to ensure that there are proper arrangements in place for oversight and effective management including the appointment of 'Handlers' and 'Controllers'. These arrangements must be specified in the application form by the applicant.

'Handler' has day to day responsibility for dealing with the CHIS. This includes directing the CHIS' day to day activities, recording the information provided, and monitoring the CHIS' security and welfare.

'Controller' responsible for the management and supervision of the 'Handler' and has general oversight of the use of the CHIS.

Authorising Officers must ensure that a risk assessment has been carried out to determine the risks to the CHIS from carrying out the task and the likely consequences should the role of the CHIS become known. Ongoing security and welfare issues should also be considered from the outset.

The 'authorisation' to carry out/conduct a CHIS operation lasts for 12 months. However, whether the operation is carried out or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, the forms do not expire. The Authorisations have to be reviewed, renewed and/or cancelled once they are no longer required. The Authorising Officer who granted or renewed the authorisation must cancel it if they are satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation or the arrangements for the CHIS no longer satisfy the requirements described in the Act.

Further guidance on CHIS can be found in the Home Office's Code of Practice on surveillance and Home Office Guidance.

Public volunteers

In some cases, a source will not establish or maintain any relationship and many sources simply provide information they have observed or acquired other than through a relationship. In this case they are not a CHIS for the purposes of RIPA and no CHIS authorisation is required.

Professional or statutory duty

In some cases, a person will be required to provide information out of a professional or statutory duty. Any such professional or statutory disclosures should not usually result in these individuals meeting the definition of a CHIS.

Tasking not involving relationships

Where tasking does not require a person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought, or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

9. ROLES AND RESPONSIBILITIES

Designated Role	Designated Officer	Responsibility
Senior Responsible Officer (SRO)	SIRO (Assistant Chief Fire Officer)	For compliance with the Act and the integrity of the process in place
Authorising Officers[2]	Head of Corporate Assurance Head of Digital Services	Granting authorisation of direct surveillance, in accordance with the Act.
RIPA Co-ordinating Officer	Senior Corporate Assurance Officer	1. Maintaining the RIPA Register and collating the original applications / authorisations, reviews, renewals and cancellations. 2. Oversight of submitted RIPA documentation. 3. Organising a RIPA training programme. 4. Raising RIPA awareness within HFRS.
Covert Human Intelligence Source (CHIS) Controller	Head of Function whose request it falls under	Management and supervision of the 'handler' and general oversight of the use of a CHIS.
Covert Human Intelligence Source (CHIS) Handler	To be determined by the Head of Function whose request it falls under	Day to day responsibility for, dealing with a CHIS, directing the activities, recording the information supplied by a CHIS and monitoring a CHIS health and welfare.

10. AUTHORISATION PROCEDURES CHIS/DIRECTED SURVEILLANCE

[2] This role must be designated to a group manager/Head of Function or higher - see schedule 1 of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010/521

Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised. Any activity under RIPA must be in strict accordance with the terms of the authorisation.

Step 1	Investigating officers consider whether the use of a covert investigation technique is necessary and proportionate. Self-assessment could show that covert investigation is avoidable as alternatives are available. If so, the matter ends and no application is made.
Step 2	If covert investigation is necessary and proportionate an application form will need to be completed.
Step 3	Applications for authorisation are to be made by Station Manager/Grade 11/12 and above to the Authorising Officers
Step 4	Before completing the application, the officer will need to obtain a unique reference number from the RIPA Co-ordinating Officer.
Step 5	The Authorising Officer will decide whether to authorise 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. Consideration must be given to the relevant codes of practice and the necessary and proportionate test.

11. DURATION OF AUTHORISATIONS

Authorisations must be reviewed in the time stated and cancelled once no longer needed. The ‘authorisation’ to carry out surveillance lasts for three months for Directed Surveillance, and 12 months (from authorisation) for a CHIS. However, whether the surveillance is carried out or not, within the relevant period will not mean the ‘authorisation’ is ‘spent’. The Forms do not expire, and they must be reviewed, renewed and/or cancelled if no longer required. Authorisations and renewals must have prior court approval.

Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including considering the benefits of the surveillance to date, and any collateral intrusion that has occurred. A court order must be obtained. The renewal will begin on the day when the authorisation would have expired.

12. WORKING WITH/THROUGH OTHER AGENCIES

When another agency has been instructed on behalf of HFRS to undertake any action under RIPA, this document and the Home Office Forms must be used (as per normal procedure) and the other agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

If in doubt, please consult with the RIPA Co-ordinating Officer at the earliest opportunity.

13. THE USE OF SOCIAL MEDIA

Paragraphs 3.10 - 3.17 of the August 2018 Covert Surveillance and Property Interference Revised Code of Practice provides detailed guidance on the use of social media for the purposes of covert surveillance.

Public authorities may use publicly available online information for legitimate statutory purposes without RIPA authorisation where activity is limited to general or preliminary checks. However, **directed surveillance authorisation should be considered** when online activity covertly focuses on specific individuals or groups, is repeated or systematic, obtains and records private information, builds a profile or pattern of life, combines information from different sources, or captures information about third parties.

The fact that information is publicly accessible may reduce, but does not automatically remove, an individual's expectation of privacy. Undisclosed online engagement may also require **CHIS authorisation**. The purpose, scope and intrusiveness of the activity are key, and the same considerations apply where searches are carried out using automated tools or by a third party on the authority's behalf.

14. TRAINING

Training will be organised by the RIPA Co-ordinating Officer.

The RIPA Co-ordinating Officer will coordinate training/refresher training as appropriate to relevant Authorising Officers, the SRO, other relevant senior managers and investigation officers where necessary.

15. RECORDS MANAGEMENT

HFRS will keep a detailed copy of all authorisations, cancellations, rejections and renewals (all renewals must have prior court authorisation). A RIPA Register of all requests and their outcome will be maintained and monitored by the RIPA Co-ordinating Officer or in their absence the Head of Corporate Assurance.

A report will be submitted annually to the Governance, Audit and Scrutiny Committee detailing the number of requests submitted for that period.

The following documents must be retained by the RIPA Co-ordinating Officer or in their absence the Head of Corporate Assurance for such purposes:

(a) a copy of the forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
(b) a record of the period over which the surveillance has taken place;
(c) the frequency of reviews prescribed by the Authorising Officer;
(d) a record of the result of each review of the authorisation;
(e) a copy of any renewal of approval of an authorisation, together with the supporting documentation submitted when the renewal was requested;
(f) the date and time when any instruction was given by the Authorising Officer, and
(g) the Unique Reference Number for the authorisation (URN).

Each form will have a URN. URNs are obtainable from the RIPA Co-ordinating Officer. Rejected Forms will also have URNs.

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 Officer should ensure an appropriate officer is designated with responsibility to ensure confidentiality, such as manage permissions and communications accordingly. For a CHIS the following must also be recorded:

(a) the actual identity of the CHIS;
(b) the identity used by the CHIS if any
(c) any other investigating authority involved, and how that authority identifies the CHIS;
(d) any information significant to the security and welfare of the CHIS;
(e) any confirmation by an officer authorising a CHIS 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.[3]

HFRS will retain original records for a period of 3 years from the ending of the authorisation.

Material obtained through covert surveillance (along with any copy of that material) must be handled and stored securely in order to minimise the risk of loss or theft. Any storage must be in such a way that makes it inaccessible to any person not authorised to access the material. Material should only be copied to the extent that a copy is necessary. In this context the term copy means entire copies of the full material and also includes any extract or summary which identifies the product of any covert surveillance. The term ‘copy’ also includes any record howsoever arising which refers to the covert surveillance or to the identities of any person to whom the material relates.

Material obtained through the use of a covert surveillance technique, along with any copy, should be securely deleted and destroyed as soon as it is no longer required. Any decision to retain material should be reviewed at least every 6 months in consultation with the SRO and RIPA Co-ordinating Officer. If following a review, there is no valid reason for its retention the material should be deleted/ destroyed.

[3] A full list of the particulars to be recorded can be found in The Regulation of Investigatory Powers (Source Records) Regulations 2000

16. INVESTIGATORY POWERS COMMISSIONER (IPC)

The Investigatory Powers Commissioner (IPC) provides independent oversight of the use of investigatory powers. HFRS will cooperate fully and promptly with any request, inspection or investigation undertaken by or on behalf of the IPC. This includes providing timely access to relevant records, authorisations, policies, systems, premises and staff, responding openly and accurately to enquiries, and taking appropriate action to address any recommendations or compliance issues identified.