North Yorkshire Fire & Rescue Service

Regulation of Investigatory Powers (RIPA) Policy

TABLE OF CONTENTS

1. INTRODUCTION

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for the control and supervision of investigatory powers exercised by specified public bodies, including North Yorkshire Fire and Rescue Authority, in order to balance the need to protect privacy of individuals particularly in light of the Human Rights Act 1998.

RIPA provides a statutory basis for the procedure, authorisation and use of covert surveillance, agents, informants and undercover officers. It regulates the use of these techniques and safeguards the public from an unnecessary invasion of their privacy.

The Authority is committed to ensuring that the necessary control and supervision of investigatory powers are in accordance with RIPA and other relevant legislation.

2. PURPOSE

The purpose of this document is the dissemination of the Regulation of Investigatory Powers Act 2000 (RIPA) policy, procedures and related guidance.

3. SCOPE

The Authority requires all Service employees to be aware of its contents and to comply fully with this policy and any related policy.

4. KEY PRINCIPLES

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

RIPA introduces:

- Lawful purposes for which the investigatory powers can be used,
- Formal authorisation of the use of any of the investigatory powers,
- The means of redress for individuals in the event of lack of compliance.

RIPA sets out the procedures that must be followed before making use of:

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

Applications made by NYFRS personnel to use covert techniques covered by RIPA **must** be made using the appropriate Home Office forms and such application must be approved by one of the designated 'Authorising Officers'. Details in respect of the application, the necessary Home Office forms and the designated Authorising Officers are set out further below including the relevant links.

RIPA is available to the Authority only when carrying out its core functions as a fire and rescue authority. ***Neither the Authority nor the Service has any historical record of using their relevant investigatory powers covered by RIPA and it is not envisaged there will be a need to do so in future. The Authority is required; however, to have a policy in place to deal with that eventuality should it arise.***

The use of social networks as a means of communication may be used by public bodies for investigatory purposes and may invoke a potential for covert use. The Office of the Surveillance Commissioners consider that such social networks, although made publicly available, may be considered as private. Consequently, the repeat viewing of individual "open source" sites for the purpose of intelligence gathering and data collection should be considered within the context of the protection that RIPA affords to such activity. Therefore the activity would have to be absolutely necessary and proportionate to meet the purpose.

The Authority needs to ensure that its officers are fully aware of RIPA, the policy and procedure associated with it and provide any relevant training required.

If you require interpretation in respect of this policy, please seek further guidance from the CAO Manager and Information Governance Officer.

5. OVERVIEW

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 to act in ways that are compatible with human rights under the ECHR. Failure to do so may enable a person to seek compensation against the Authority or to use any failure as a defence in any proceedings that the Authority may bring.

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 covert surveillance, covert individuals and acquisition of communications can be used. The Authority is included in the list of public authorities which can rely on RIPA.

As detailed above, the Authority 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 the Authority will usually be able to gather all the information required for its statutory functions without covert information gathering techniques. This policy does not change this position. If the Authority were to ever use the powers under RIPA a fair balance must be drawn between the public interest and the rights of individuals.

The purpose of this document 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.

The protection of RIPA is available to the Authority only when carrying out its core functions as a fire and rescue authority. RIPA therefore does not apply to the ordinary general functions carried out by the Authority e.g. staff, staff disciplinary or contractual issues.

This document is intended to ensure that the Authority's policy, practice and procedure 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, by the Office of Surveillance Commissioners (OCS) and by the Interception of Communications Commissioners Office (ICCO). Links to documentation referred to in this Policy are shown in Appendix A, where such documentation is publicly available. Please contact the CAO Manager and Information Governance Officer, however, for the Office of Surveillance Commissioners Procedure and Guidance document December 2014.

6. ACTIVITIES AND DEFINITIONS COVERED BY RIPA

There are three forms of covert intelligence gathering that are covered by RIPA and potentially available to the Authority: (1) Directed Surveillance; (2) Covert Human Intelligence Sources and (3) Acquisition of Communications Data.

Acquisition of Communications Data is dealt with in section 11 at the end of this Policy. The Interception of Communications Commissioners' Office has oversight of the regulatory regime of this part of RIPA.

Directed Surveillance Covert Human Intelligence Sources are governed by the Office of the Surveillance Commissioners (OCS). There is an inspection of the Authority every three years as a means of external independent oversight.

(1) 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 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).

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).

Any covert surveillance of what takes place in residential premises or a private vehicle is deemed as "intrusive surveillance" and outside what the Authority may lawfully do even under RIPA. For the avoidance of doubt, **the Authority *cannot* undertake intrusive surveillance.**

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.

(2) 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 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 may be a CHIS. The Authority would owe that person a duty of care and must consider whether using the information provided might place the person 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. 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.

7. WHEN RIPA PROCEDURES CAN BE USED

The covert intelligence gathering techniques under RIPA can be used only in certain prescribed circumstances. For the Authority these are where:

(a) their use is necessary for:

- the prevention or detection of crime;
- preventing disorder; or
- in the interests of public safety;

and

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

In addition, 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.

RIPA can be relied on only in carrying out the Authority's 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.

In deciding whether the “necessary and proportionate” test is passed, authorising 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.

8. AUTHORISATION PROCESS

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

The first step is for investigating officers to consider for themselves whether the use of a covert investigation technique is necessary and proportionate. 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.

If it continues to appear covert surveillance is necessary and proportionate an application for approval should be made on the appropriate Home Office form. The links to each individual Home Office form as part of the authorisation process are contained within Appendix A.

Applications for authorisation are to be made by Station Manager and above to the Authority's designated relevant RIPA Authorising Officers.

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 or practice and the necessary and proportionate test.

No covert surveillance can begin until this written authorisation is issued.

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

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

In addition, when granting authorisation 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 authorisation should not last longer than is justified by the "necessary and proportionate" test and an authorisation must 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.

At the expiry of an authorisation it must be formally cancelled by the Authorising Officer and not simply allowed 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.

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. The handler will report to directly to an individual appointed as a "controller", who will monitor and supervise the management of the use of the CHIS, therefore providing further oversight and scrutiny

Officers seeking a CHIS authorisation 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 authorisation in accordance with record keeping below.

The Authorising Officer **will not authorise 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.

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 are also in place.

The Protection of Freedoms Act 2012 requires certain local authorities, once they have approved RIPA authorisation internally, to then obtain judicial approval to that authorisation. The definitions of "local authority" contained in that Act, however, do NOT extend to combined fire and rescue authorities and so this stage is not required for any RIPA authorisation granted in accordance with this policy prior to the covert surveillance commencing.

9. RECORD KEEPING

The Senior Responsible Officer (SRO), Director of Finance and Technical Services (Treasurer) is the senior manager with oversight of compliance with RIPA. The SRO has overall responsibility for:

a) the integrity of the policy for managing RIPA;

b) 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.

A specific area has been created whereby Authorising Officers must;

(i) retain a copy of every completed form in respect of each:

- authorisation approved by them
- review
- renewal; and
- cancellation

(ii) 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, for directed and five years for CHIS. This register must also include applications refused, stating the reasons for any refusal.

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. The following must also be recorded (and records retained for at least five 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 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.

All information is to be classified as OFFICIAL-SENSITIVE and only accessed by those that are involved in that particular case and what is relevant.

10. ROLES

Roles required to comply with Directed Surveillance and CHIS aspects of the Act:

Senior Responsible Officer (SRO) for RIPA (Director of Finance and Technical Services) (Treasurer) is responsible for compliance with the Act and the integrity of the process in place.

RIPA Co-ordinating Officer (Head of Finance and Administration), is responsible for, (a) maintaining the Central Record of Authorisations and collating the original applications / authorisations, reviews, renewals and cancellations; (b) oversight of submitted RIPA documentation; (c) organising RIPA training programme; and (d) raising RIPA awareness in NYFRS.

Authorising Officers (Direct Surveillance) (Group Manager Staff Risk and Group Manager Prevention and Protection) are responsible for granting authorisation of direct surveillance, in accordance with the Act. Only the Secretary of State can give authorisation to carry out intrusive surveillance.

Authorising Officers (CHIS) (Group Manager Staff Risk and Group Manager Prevention and Protection), is responsible for granting authorisation of CHIS surveillance, in accordance with the Act.

CHIS Handler (Nominated Station Manager) will have day to day responsibility for, dealing with the CHIS, directing the activities, recording the information supplied by the CHIS and monitoring the CHIS health and welfare. The record keeping will be in accordance with RIP (Source Record) Regulations SI2000/2725 as detailed in section 9 (a –k).

CHIS Controller (Nominated Group Manager or above), will be responsible for the management and supervision of the 'handler' and general oversight of the use of the CHIS. The record keeping will be in accordance with RIP (Source Record) Regulations SI2000/2725 as detailed in section 9 (a –k)

11. ACQUISITION OF COMMUNICATIONS DATA

The acquisition of communications data is under review so the guidance below is subject to change. In the draft Investigatory Powers Bill published 4th November 2015, the Government plans to restrict the power of fire and rescue services to acquire communications data to only 'threat to life' situations.

Until further notice, in order to acquire communications data from Communications Service Providers (CSP's), the Authority must make use of a Home Office accredited SPoC. North Yorkshire Fire and Rescue Authority does not have an accredited SPoC, therefore do not have the ability to utilise this element of RIPA, however for reference purposes the process of acquiring this type of data has been set out below.

A third technique of covert investigation available to Fire and Rescue Authority's under RIPA, is 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 acquire this data. The communications

data that can be obtained by fire authorities is strictly limited and appropriate to the situation or investigation being managed.

Communication Data is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written).

During the management of an on-going emergency the control room may acquire all types of communications data if required 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;

Under other legislation, systems and processes for this information is supplied when dealing with emergency situations, with no requirement to use RIPA. The Public Emergency Communications Service Code of Practice recognises that an emergency period of one hour after termination of the emergency call in which disclosure of communications data to emergency services will largely fall outside the provisions of RIPA (the golden hour rule).

However, once an emergency has passed, or if there is an on-going investigation over a period of time, then for

a) the purpose preventing or detecting crime, or preventing disorder, or,
b) in the interests of public safety,

Communications data consisting of subscriber information or service use data may be acquired as long as the amount, type, and nature of the data acquired is necessary and proportionate in the circumstances. Below are examples provided within the Acquisition of Communications Data Code of Practice.

(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.

The Authority could not access the content of an individual's communications.

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.

The SPoC is responsible for facilitating the handover of any data in accordance with the law including new statistical requirements required to be kept from 1 January 2015 in relation to the Acquisition and Disclosure of Communications Data under Part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA).

The SPoC will review the authorisation from the Designated Person 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
(c) If the acquisition should be by use of a notice or authorisation

If satisfied of these the SPoC returns the application to the Designated Person for authorisation.

Only if the acquisition has been authorised, 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.

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 Service policy on data protection.

12. POLICY GOVERNANCE

The following table identifies who within North Yorkshire Fire & Rescue Service is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
  N.B Only **one** role is held accountable.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	IGG, Director of Finance and Technical Services (Treasurer)
Accountable	Chief Fire Officer / Chief Executive

Consulted	IGG
Informed	All Employees, All Temporary Staff, All Contractors

This is an electronic version of the approved version and paper copies are only valid as of the last update. Please refer to the master copy or the document author if you are in any doubt about the document content.

13. REFERENCES

Internal:

- Data Protection Policy
- Staff Code of Conduct
- Social Media Policy
- Visual Imaging Policy

External:

- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Protections of Freedoms Act 2012
- RIPA Home Office Code of Practice and Forms
- The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) 2010 and amended 2012
- The Regulations of Investigatory powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2013

* * * * * * * * * *

If you have any questions concerning this policy or your obligations under it, you may direct them to either your line manager or contact the Service on 01609 780150.

North Yorkshire Fire & Rescue Service

Thurston Road

Northallerton

North Yorkshire

DL6 2ND

Appendix A – Reference Material and Forms

Surveillance Commissioners:

Office of Surveillance Commissioners

Office of Surveillance Commissioners Annual Report 2014

Office of Surveillance Commissioners Annual Report 2015

Office of Surveillance Commissioners Procedures and Guidance Document December 2014 (NOTE: this is a restricted publication document – please contact the CAO Manager and Information Governance Officer)

Interception of Communications Commissioner's Office:

Interception of Communications Commissioner's Office

Codes of Practice:

Codes of Practice

Investigatory Powers Tribunal:

Investigatory Powers Tribunal

Investigatory Powers Tribunal Judgments

Forms:

Directed Surveillance

Application for the Use of Directed Surveillance

Renewal Of Directed Surveillance

Review of the Use of Directed Surveillance

Cancellation of the Use of Directed Surveillance

Covert Human Intelligence Sources

Application for the Use of Covert Human Intelligence Sources

Renewal Of Authorisation to Use Covert Human Intelligence Sources

Reviewing the Use of Covert Human Intelligence Sources

Cancellation of Covert Human Intelligence Sources

Reporting errors to the IOCCO:

Reporting an Error by a CSP to the IOCCO

Reporting an Error by a Public Authority to the IOCCO

Appendix B – FLOWCHART

RIPA Directed Surveillance Decision Chart – Home Office Code