DEVON & SOMERSET FIRE & RESCUE SERVICE

Corporate Services Dept.
Service Policy Document

Summary of Main Changes:-

The main changes to this policy are as a result of:

- Codes of Practice providing guidance on the Regulation of Investigatory Powers Act 2000 for Covert Surveillance and Property Interference and Covert Human Intelligence Sources approved by parliament on 10 December 2014
- Office of Surveillance Commissioners Annual Report 2013-2014 and, in particular, covert use of social media for investigations
- Office of Surveillance Commissioners Procedures and Guidance December 2014
- Change of ownership of the policy from Corporate Communications to Corporate Services
- Revisions recommended from 2015 Office of Surveillance Commissioner's (OSC) Inspection incorporated
- Incorporation of comment on implications for acquisition of communications data of the Investigatory Powers Act 2016

DEVON & SOMERSET FIRE & RESCUE SERVICE

Corporate Services Dept.
Service Policy Document

Document Purpose:-

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

NOTE – If you are reading a paper copy of this document it may not be the most up to date version. For the latest version view the information on the Service website or intranet.

Document Status:-

Ownership:	Corporate Services
Originating Date:	December 2014
Review Date:	January 2018
Next Review or Amendment:	April 2019
Key Consultees:	Executive Board

Further Information:-

Mike Pearson
Director of Corporate Services
mpearson@dsfire.gov.uk

Cross-References:-

Appropriate Use of Social Media and Electronic Communications DSFRS Policy
Regulation of Investigatory Powers Act 2000
Human Rights Act 1998
Data Protection Act 1998
Freedom of Information Act 2000
The Regulation of Investigatory Powers (Communications) Order 2003
Protection of Freedoms Act 2012
The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012
The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2013
The Investigatory Powers Act 2016

POLICY STATEMENT

A. 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 Devon & Somerset Fire & Rescue Service (the Service), in order to balance the need to protect privacy of individuals particularly in light of the Human Rights Act 1998.

B. 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.

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

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

COMPLIANCE STATEMENT

A. The Authority will not discriminate against any persons in the application of this policy or any subordinate procedures.

B. This policy is OPEN under the Freedom of Information Act 2000.

KEY INFORMATION

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

B. 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

C. 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

D. Please note applications to use covert techniques covered by RIPA must be made using the appropriate Home Office forms in conjunction with a completed risk assessment and such application must be approved by one of the designated relevant 'Authorising Officers'. Further 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.

E. 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.

F. 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.

G. 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.

H. If you require interpretation in respect of this policy, please seek further guidance from the Director of Corporate Services, the Democratic Services & Corporate Support Manager or the Corporate Communications Manager.

CONTENTS

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 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.

1.2. 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, these rules 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.

1.3. As noted 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 was to ever use the powers under RIPA a fair balance must be drawn between the public interest and the rights of individuals.

1.4. 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.

1.5. The protection of RIPA is available to the Authority 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 the Authority e.g. staff disciplinary or contractual issues. Another legal basis for avoiding infringing rights to privacy would be needed in those circumstances and for non-RIPA surveillance the Authority has in place a similar process to document consideration of human rights principles in the interests of professional and ethical investigation, fairness and transparency.

1.6. 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 the appendix, where such documentation is publicly available.

2. ACTIVITIES AND DEFINITIONS COVERED BY RIPA

2.1 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.

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

2.3 The Interception of Communications Commissioners' Office (ICCO) has oversight of the regulatory regime of this part of RIPA. The acquisition of Communications Data is dealt with in section 7 on page 14 at the end of this policy.

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).

2.4 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).

2.5 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.

2.6 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. Covert 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.

Covert Human Intelligence Sources

2.7 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.

3. WHEN RIPA PROCEDURES CAN BE USED

3.1 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. The RIPA regime is concerned only with the regulation of certain investigatory powers and not with "ordinary functions" such as the regulation of employees or of suppliers and service providers.

Necessity

3.2 Prior to authorising any request for covert surveillance under RIPA, an Authorising Officer must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in Section 28(3) of RIPA (the "necessity" test). For a fire and rescue authority, these purposes are:

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

To satisfy the necessity test, the conduct which the covert surveillance is intended to prevent or detect **must** be identified and clearly described in both the application and the authorisation.

Proportionality

3.3 The "proportionality" test is a key concept of RIPA. It is a critical judgement that can only properly be reached once all other aspects of an authorization have been fully considered. Proportionality is about:

- Balancing the effectiveness of covert over overt methods; ***and***
- Explaining why the particular covert method, technique or tactic is most appropriate.

3.4 In authorising a request for covert surveillance, an Authorising Officer **must** clearly record and evidence how they have reached the conclusion that that the activity is proportionate to what it seeks to achieve, including an explanation of the reasons why the method, technique or tactic proposed is not disproportionate (the proverbial "sledgehammer to crack a nut"). It will be insufficient to make a simple assertion or say that the seriousness of the issue justifies any or every method available. Similarly, it may be unacceptable to advance lack of resources or a potential cost saving as sufficient grounds to use a technological solution which could be more intrusive than a human being.

3.5 A methodical approach must be adopted to satisfy the "proportionality" test involving:

(a) consideration of 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) and providing evidence of other methods considered and why they were not implemented;

(b) demonstrating that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result;

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

(d) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others (see also collateral intrusion below)

(e) considering 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.

Collateral Intrusion

3.6 Every effort must be made to avoid or minimise "collateral intrusion" i.e. 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.

3.7 All applications for authorisation must include an assessment of the risk of collateral intrusion and details steps to be taken either to avoid entirely or minimise any collateral intrusion. This assessment should include consideration of the following factors:

- Timing of the surveillance;
- Amount of surveillance;
- Method of surveillance;
- Sensitivities of the local community; and
- Operations by other public authorities.

3.8 The Authorising Officer must take account of the assessment when considering the proportionality of the proposed surveillance.

3.9 Finally, it must be stressed that 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 also comply with all relevant Codes of Practice, Procedures and Guidance Notes.

4. THE AUTHORISATION PROCESS

Authorisation 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 authorisation approval in place. This authorisation 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 by way of a risk assessment should be made and retained by the investigating officer.

4.3 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.

4.4 If it continues to appear covert surveillance is necessary and proportionate an application for approval should be made only by designated RIPA Applicants 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.

4.5 Applications for authorisation are to be made to the Authority's designated relevant RIPA Authorising Officers.

4.6 Applicants should complete the relevant application form and then submit this initially to either the RIPA Co-ordinator or the Senior Responsible Officer (SRO) for quality assurance purposes. Only after feedback has been received and actioned (in consultation with the RIPA Co-ordinator/SRO as necessary) on the proposed application should it then be submitted for authorisation.

4.7 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.

4.8 Authorisations should normally be in writing except that in urgent cases they may be given orally by an Authorising Officer. A case will only be urgent if the time taken to apply in writing would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the Authorising Officer's or applicant's own making.

4.9 With the exception of urgent, oral authorisations (see paragraphs 4.8 and 4.10), once an authorisation has been granted this should be forwarded to either the RIPA Co-ordinator or the SRO for quality assurance purposes. The authorised activity should only commence once the Authorising Officer has received feedback on the authorisation from the RIPA Co-ordinator or the SRO (and has actioned any feedback as necessary following feedback from the RIPA Co-ordinator or SRO).

4.10 All urgent, oral authorisations must subsequently be recorded in writing, as soon as is reasonably practicable after the authorisation, by both the Authorising Officer concerned and the applicant. This written record should include those details that would otherwise be required for a written application. The Authorising Officer should also ensure that details of the urgent oral authorisation are entered on the Central Register.

4.11 Details of designated RIPA Applicants and Authorising Officers can be found at Appendix B to this document.

NO COVERT SURVEILLANCE CAN BEGIN UNTIL AUTHORISED IN WRITING (OR, IN URGENT CASES ONLY, ORALLY)

4.12 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 at 23.59hours)
CHIS -	12 months (less one day at 23.59hours)

4.13 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.

4.14 Authorisations **must** be cancelled, formally, by the Authorising Officer as soon as the need for the covert surveillance no longer exists – authorisations should 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.

4.15 Additionally, when authorising a CHIS the Authorising Officer must ensure before granting an authorisation that the following roles are in place:

- a “handler” who 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;
- a “controller” responsible for management and supervision of the “handler” and who also has general oversight of the use made of the source, therefore providing further oversight and scrutiny; and
- an individual responsible for maintaining records of each source, the records to contain those particulars as specified in regulations made by the Secretary of State (currently the Regulation of Investigatory Powers [Source Records] Regulations 2000 [SI 2000/2725]). For the avoidance of doubt, legal advice should be sought during any CHIS application process as to the “source records” to be maintained.

4.16 Officers seeking a CHIS authorisation must 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.

4.17 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.

4.18 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.

4.19 For the avoidance of doubt, 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.

5. RECORD KEEPING

5.1 The Senior Responsible Officer (SRO) is a 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.

5.2 Authorising Officers must:

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

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

(ii) pass ***the originals of each of the above forms*** to the RIPA Co-ordinator 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 For a CHIS, records must be securely stored separately from other documentation. The records must be retained for at least five years and should contain the following information:

a) the actual identity of the CHIS;

b) the identity used by the CHIS if any;

c) the unique identifying reference number (and code name, if applicable) used for the CHIS;

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

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

f) 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;

g) when and how the CHIS was recruited;

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

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

j) all contacts and communications between the source and the handler;

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

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

5.4 The originals of these records should be passed as soon as is practicable to the RIPA Co-ordinator who will maintain a centrally retrievable record of CHIS authorisations identifying the following:

a) The unique reference number of the CHIS and any code name that may have been applied;

b) The date the authorisation was granted, renewed or cancelled;

c) An indication of whether the activities were self-authorised.

6. OVERSIGHT AND REVIEW

6.1 The SRO maintains general oversight of the Authority's use of RIPA and compliance with legal requirements and the codes of practice.

6.2 The Surveillance Commissioners and Interception of Communications Commissioner provide external oversight and from time to time may inspect the Authority's policies, procedures 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.

6.3 In accordance with those codes, the Authority is required to review the policy on the use of RIPA at least annually, with this review to include details (in an anonymised form) of any use by the Authority of RIPA. This is to ensure the Authority is able to judge whether the policy is being applied appropriately. For the avoidance of doubt, individual Members of Authority have no role in authorising or refusing any particular application to use RIPA procedures.

7. ACQUISITION OF COMMUNICATIONS DATA

NOTE: The Investigatory Powers Act 2016 contains provisions to restrict, for fire and rescue authorities, authorisations to acquire communications data to only those purposes necessary to prevent 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. Although the Act has received Royal Assent, at the date of drafting this document the Commencement Order to bring these provisions into force had not been made. Consequently, prior to making any application for the acquisition of communications data, further advice should be sought of the current legal position.

7.1 A third technique of covert investigation available to the Authority under RIPA is communications data. 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).

7.2 Postal or Communications Service Providers (CSPs) 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.

7.3 During the management of an ongoing emergency the control room may acquire, without RIPA authorisation, any communications data required to prevent death or injury or any damage to a person's physical or mental health, or to mitigate any injury or damage to a person's physical or mental health.

7.4 Additionally, the Public Emergency Communications Service Code of Practice provides that caller location information not previously supplied (but which would otherwise have been available) may be requested of CSPs for up to one hour after the original emergency call without the need for RIPA authorisation (the "golden hour" rule).

7.5 Once the emergency has passed, however (or if there is an ongoing 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 from a CSP as long as the amount, type, and nature of the data acquired is necessary and proportionate in the circumstances.

7.6 The Acquisition of Communications Data Code of Practice cites the following as examples of subscriber information and service use data:

(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.

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

Process for the Acquisition of Communications Data.

7.8 This features three roles:

1. The Applicant;
2. The Authorising Officer; and
3. A Senior Point of Contact (SPoC)

Each of these roles should be carried out by a different person.

The Applicant

7.9 This is the person involved in conducting an investigation or operation who makes the application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the Authorising Officer, the necessity and proportionality of a specific requirement for acquiring communications data.

The Authorising Officer

7.10 The Authorising Officer is the individual responsible for considering and authorising any application made for the acquisition of communications data.

7.11 In doing so, the Authorising Officer will assess necessity and proportionality (including the potential for unintended consequences) of the application. Before granting the application, the Authorising Officer must take account of advice provided by the SPoC.

7.12 In discharging the role of Authorising Officer, it is important that the individual concerned is independent of any operation or investigation related to the application.

The Senior Point of Contact (SPoC)

7.13 To acquire communications data from a CSP, the Authority must make use of a Home Office accredited SPoC

7.14 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.

7.15 The accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for the acquisition of communications data are undertaken. The role of the SPoC is to provide objective judgement and advice to both the Applicant and Authorising Officer and in so doing provides a “guardian and gatekeeper” function ensuring that the Authority acts in an informed and lawful manner.

7.16 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).

7.17 The SPoC will review the application and consider whether:

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

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

(c) If the acquisition should be by use of a notice or authorisation

7.18 If satisfied of these the SPoC returns the application to the Authorising Officer for authorisation.

7.19 ***Only when the acquisition has been authorised*** will the SPoC prepare a Notice in the form prescribed by the Home Office to serve on the CSP. The CSP will provide the data to the SPoC.

7.20 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.

APPENDIX A

Surveillance Commissioners

Office of Surveillance Commissioners

Office of Surveillance Commissioners Annual Report 2014

Interception of Communications Commissioner's Office

Interception of Communications Commissioner's Office

Codes of Practice, Procedures and Guidance

Codes of Practice

Office of the Surveillance Commissioners Procedures and Guidance

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

Designated Officers

Applicants

Paul Bray	Community Safety Protection Manager
Michelle Purchase	Business Safety Officer
Wendy Endacott	HR Operations Manager
Karen Harding	HR Officer (Operations)

Authorising Officers

Darren Peters	Area Manager
Joe Hassell	Area Manager
Sarah Allen	Area Manager
Steven Pope	HR Manager

CHIS Authorising Officers

Glenn Askew	Chief Fire Officer
Alex Hanson	Assistant Chief Fire Officer *
Peter Bond	Assistant Chief Fire Officer *

*in the absence of the Chief Fire Officer and/or as delegated by the Chief Fire Officer

Senior Responsible Officer (SRO)

Mike Pearson	Director of Corporate Services
Steve Yates	Democratic Services & Corporate Support Manager **

** in the absence of the Director of Corporate Services and/or as delegated by the Director of Corporate Services

RIPA Co-Ordinator

Steve Yates	Democratic Services & Corporate Support Manager

Single Point of Contact (SPoC)

Tieneka Akers	Corporate Communications Manager

APPENDIX C

RIPA Directed Surveillance Decision Chart