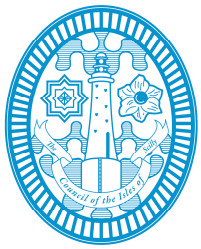
Regulation of Investigatory Powers Act 2000

Corporate Surveillance Guidance



Council of the
ISLES OF SCILLY

May 2015

Version	1.3	**Approving Committee**	Full Council
Date	7th March 2013	**Ratified by Council**	7th March 2013
Responsible Officer	Sue Pritchard	**Review Date**	

Version History			
Date	**Version**	**Author/Editor**	**Comments**
7th March 2013	1.3	Sue Pritchard	Version 3 approved by Council following review
14th May 2015	1.4	RNB	Addition of version control and minor updating following new Code of Practice July 2014

Equalities Impact Assessment Record					
Date	**Type of Assessment Conducted**	**Stage/Level completed (where applicable)**	**Summary of Actions Taken Decisions Made**	**Completed by.**	**Impact Assessment Review date**

Document retention	
Document retention period	

CORPORATE SURVEILLANCE GUIDANCE

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Summary

The Regulation of Investigatory Powers Act 2000 ('RIPA') brought into force the regulation of covert investigation by a number of bodies, including local authorities. RIPA regulates a number of investigative procedures, the most recent of which is the access to communications data. This document is intended to provide officers with guidance on the use of covert surveillance, Covert Human Intelligence Sources ('Sources') and the obtaining and disclosure of communications data under RIPA. Officers must take into account the Codes of Practice issued under RIPA (RIPA and the Codes of Practice may be found at www.security.homeoffice.gov.uk).

1.2 Background

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his home and his correspondence. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:

(a) in accordance with the law

(b) necessary (as defined in this document); and

(c) proportionate (as defined in this document)

RIPA provides a statutory mechanism for authorising certain types of surveillance. 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, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the council could be ordered to pay compensation. It is essential, therefore, that all involved with RIPA comply with this document and any further guidance that may be issued, from time to time, by the Solicitor to the Council.

Each officer of the Council with responsibilities for the conduct of investigations, shall, before carrying out any investigation involving RIPA, undertake appropriate training to ensure that investigations and operations that he/she carries out will be conducted lawfully.

The Chief Executive is appointed as the senior responsible officer to ensure the integrity of the process within the Council and its compliance with RIPA; to have oversight of reporting of errors to the relevant oversight commissioner; responsibility for engagement with the office of Surveillance Commissioners when they conduct their inspections and where necessary, oversight of the implementation of any post-inspection action plan. The senior responsible officer will also ensure that Members regularly review the Council's use of RIPA. Delegation to the Senior Officer: Democratic and Licensing will occur, but regular reports of activity will be presented to the Management Team and subsequently to Members. The Senior Officer: Democratic and Licensing is an Authorising Officer.

1.3 Review

RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to surveillance. This document will, therefore be kept under yearly review by the Chief Executive. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Chief Executive at the earliest possible opportunity.

1.4 Scope

RIPA covers the authorisation of directed surveillance, the authorisation of sources and the authorisation of the obtaining of communications data. Communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, contents of e-mails or interaction with websites. An authorisation under RIPA will provide lawful authority for the investigating officer to carry out surveillance.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Data Protection Act 1998. RIPA forms should be used where **relevant** and they will only be relevant where the **criteria** listed on the forms are fully met.

2. GENERAL

2.1 Definition of Surveillance

'Surveillance' includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device.

Surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

2.2 Confidential Material

Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information, confidential journalistic material and communications between an MP and a constituent.

Applications in which the surveillance is likely to result in the acquisition of confidential material will only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The Authorising Officer shall give the fullest consideration to any cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his or her home.

Where a likely consequence of surveillance would result in the acquisition of confidential material, the investigating officer must seek authority from the Chief Executive, or, in his absence, the Section 151 Officer **and** the Senior Officer: Democratic and Licensing.

2.3 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, which came into force on 1 November 2012 imposes further restrictions on local authorities use of RIPA. It restricts Authorising Officers from authorising the carrying out of directed surveillance unless it is for the purpose of preventing or detecting a criminal offence unless the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment or constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

3 DIRECTED AND INTRUSIVE SURVEILLANCE

3.1 Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

3.2 Intrusive Surveillance

That surveillance becomes intrusive if the covert surveillance:

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; or

b) is carried out without that device being present on the premises or in the vehicle, is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle, or

c) is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations

Therefore directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device OR when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

For intrusive surveillance relating to residential premises or private vehicles, if any device used is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

Where covert surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

Currently, local authorities are **not** authorised to carry out intrusive surveillance.

4 IDENTIFYING DIRECTED SURVEILLANCE

Ask yourself the following questions:

4.1 Is the surveillance covert?

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, Officers will be behaving in the same way as a normal member of the public (eg in the case of most test purchases), and/or will be going about Council business openly (eg a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (eg where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that conditions are being met.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

4.2 Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be

occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.3 Is the surveillance in such a manner that is likely to result in the obtaining of private information about a person?

Private information includes any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.4 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5 COVERT HUMAN INTELLIGENCE SOURCES

5.1 Definition

A person is a source if:

a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

b) they covertly use such a relationship to obtain information or to provide access to any information to another person; or

c) they covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A source may include those referred to as agents, informants and officers working undercover.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

This covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (eg walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

The Code of Practice states that the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources. It should be noted however that an informant, albeit not tasked to obtain information on behalf of the council, could nevertheless fall with the definition of a CHIS if he has obtained the information in the course of, or as a result of the exsistence of, a personal or other relationship. In other words it is "inside information" as opposed to information obtained through outside observation. In these instances a duty of care will arise when considering how the information should be used.

The Protection of Freedoms Act 2012. Section 38 of that Act came into force on 1st November 2012. That provision amends the Regulation of Investigatory Powers Act 2000 to require that, where an Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of covert human intelligence sources, judicial approval will be required.

On receipt of an application for the use of covert human intelligence the Chief Executive will then make arrangements for an application to be made to the Magistrates Court.

5.2 Security and Welfare

Only the Chief Executive or, in his absence, the Section 151 Officer is able to authorise the use of vulnerable individuals and juvenile sources. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile

sources, more particularly set out in the Covert Human Intelligence Source Code of Practice at www.security.homeoffice.gov.uk.

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

6 COMMUNICATION DATA

6.1 Definition

This covers any conduct in relation to a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

Communications data includes subscribers details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc.

Two types of data (Customer Data or Service Data) are available to local authorities and, when making an application for obtaining or disclosing such data, the applicant must specify exactly which type of information is required from within each of the subscriber data and service use data.

a) Customer data – (Subscriber data, RIPA s21(4))

Customer data is the most basic. It is data about users of communication services.

This data includes:

- Name of subscriber
- Addresses for billing, delivery, installation
- Contact telephone number(s)
- Abstract personal records provided by the subscriber (e.g. demographic information)
- Subscribers' account information – bill payment arrangements, including bank, credit/debit card details

- Other services the customer subscribes to.

b) Service data – (Service Use data, RIPA s21(4)(b))

This relates to the use of the service provider's services by the customer, and includes:

- The periods during which the customer used the service(s)
- Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers
- 'Activity', including itemised records of telephone calls (numbers called), internet connections, dates and times/duration of calls, text messages sent
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection
- 'Top-up' details for prepay mobile phones – credit/debit card, voucher/e-top up details

A third type of data (traffic data) is not accessible to local authorities.

6.2 Social Media Site investigation

The viewing of open source material does not require authorisation unless and until it is repeated or systematic, at which stage directed surveillance authorisation should be considered.

Passing an access control so as to look deeper into a site, for example by making a "friend request", requires at least directed surveillance authorisation. If the investigator is to go further and pursue enquiries within the site, thereby establishing a relationship with the site host in the guise of a member of the public, this requires a CHIS authorisation.

7 AUTHORISATION PROCEDURE

7.1 General

Authorisation is required for the use of directed surveillance, for the conduct and use of sources and for the conduct in relation to a postal service or telecommunication system and the disclosure to any person of such data.

Any officer who undertakes investigations on behalf of the Council shall seek authorisation in writing for any directed surveillance or for the conduct and use of any source. Persons

granting an authorisation must believe that it is proportionate to what is sought to be achieved.

The Authority will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if and only if, at the date of the grant of authorisation or renewal of an existing authorisation they are satisfied that:

(a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain.

(b) the "relevant conditions" were satisfied in relation to the authorisation.

Relevant conditions include that:

(i) the relevant person was designated as an Authorising Officer.

(ii) it was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with.

(iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA (restrictions on the rank of the person granting the authorisation).

(iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

Any officer wishing to engage in conduct in relation to a postal service and telecommunication system for obtaining communications data and the disclosure to any person of such data must also seek authorisation, the procedure and procedure of which differs slightly and is outlined in paragraph 7.4.

7.2 Who can give Authorisations?

The Protection of Freedoms Act 2012. Section 38 of that Act came into force on 1st November 2012. That provision amends the Regulation of Investigatory Powers Act 2000 to require that, where an Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of covert human intelligence sources, judicial approval will be required. Oral authorisation of the use of RIPA techniques are no longer permitted for local authorities.

By law, the 'Authorising Officer' for local authority purposes is any assistant Chief Officer, assistant Head of Service, service manager or equivalent. More senior officers within a Council may also give authorisations in the circumstances to those whom they are senior. Please note that certain authorisations, namely those relating to confidential information,

vulnerable individuals and juvenile sources, can only be granted by the Chief Executive, or, in his genuine absence, the Section 151 officer together with the Senior Officer: Democratic and Licensing.

The Council's authorised posts are listed in Appendix 1. This appendix will be kept up to date by the Administration Officer in consultation with the Chief Executive and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, a request must be referred to the Chief Executive for consideration as necessary. The Chief Executive has the delegated authority to add, delete or substitute posts.

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by a recognised trainer, before Authorising Officers are certified to sign any RIPA forms. A certificate of training will be provided to the individual and a central register of all those individuals who have undergone training or a one-to-one meeting with the Chief Executive on such matters, will be kept by the Senior Officer: Democratic and Licensing.

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of any forms to the Chief Executive, the same are sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

On receiving an application for directed surveillance the Chief Executive will then make arrangements for an application to made to the Magistrates Court (see 7.1).

7.3 Grounds for Authorisation – the 'necessary & proportionate' test

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance.

An Authorising Officer shall not grant an authorisation for the carrying out of directed surveillance, or for the use of a source or for the obtaining or disclosing of communications data unless he believes:

a) that an authorisation is necessary and

b) the authorised investigation is proportionate to what is sought to be achieved by carrying it out

For local authority investigations, authorisation is deemed "**necessary**" in the circumstances of the particular case if it is

a) For the purpose of preventing or detecting a crime or preventing disorder (punishable wit at least six months imprisonment);

Conduct is not deemed "**proportionate**" if the pursuance of the legitimate aim listed above will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any conduct must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe. The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration. For example, covert surveillance relating to dog fouling and schools admissions/suspected false addresses is unlikely to be deemed a proportionate activity, though it is accepted that each case must be assessed on a case by case basis.

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities. Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

Collateral Intrusion

Before authorising investigative procedures, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for an authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

7.4 Special Procedure for Authorisation of and Issuing of Notices in respect of Communications Data

7.4.1 The Act provides two different ways of authorising access to communications data; through an authorisation under Section 22(3) and by a notice under Section 22(4). An authorisation would allow the authority to collect or retrieve the data itself. A notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority serving the notice. An Authorising Officer decides whether or not an authorisation should be granted or a notice given.

7.4.2 In order to illustrate, a Section 22(3) authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

7.4.3 Applications for the obtaining and disclosure of communications data may only be made by officers of the Council. Reference should be made to the process map at Appendix 2 for guidance as to the process to be followed.

7.4.4 Unless urgent, (see paragraph 7.5) notices and, where appropriate, authorisations for communications data must be channelled through single points of contact ("s") in the authority. The SPoC for the Council of the Isles of Scilly is the Chief Executive,: email, tleijser@scilly.gov.uk). The SPoC is able to advise authorising officers as to whether an authorisation or notice is appropriate.

7.4.5 The SPoC:

a) where appropriate, assesses whether access to the communications data is reasonably practical for the postal or telecommunications operator;

b) advises applicants and authorising officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators;

c) provides safeguards for authentication;

d) assesses the cost and resource implications to both the authorisation and postal or telecommunications operator.

7.4.6 Applications to obtain communications data should be made on the standard form at Appendix 3 and submitted in the first instance to the SpoC, and if appropriate will forward the application to the Authorising Officer for either the authorisation of conduct or the issuing of a notice. If satisfied that the proposed investigation is both necessary and proportionate, the Authorising Officer will return the authorisation or notice to the SPoC who will then liaise with the postal / telecommunications company. The disclosure of data under a notice will only be made to the authorising officer or to the Council's SPoC.

7.4.7 Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection Act 1998 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

7.5 Urgency

Urgent authorisation should not be necessary, and local authorities are no longer permitted to grant approvals orally.

7.6 Standard Forms

Authorisations must be in writing.

Standard forms for seeking directed surveillance and source authorisations are provided at Appendix 4. The authorisation shall be sought using the standard forms as amended from time to time.

Any person applying or granting an authorisation willalso need to be aware of the particular sensitivities in the local community where a covert human intelligence source is used.

8 ACTIVITIES BY OTHER PUBLIC AUTHORITIES

8.1 The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

9 JOINT INVESTIGATIONS

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

When some other agency (eg Police, Customs & Excise, Inland Revenue etc):

(a) wish to use the Council's resources (eg CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he must obtain a copy of that

agency's RIPA form for the record and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

10 DURATION, RENEWALS AND CANCELLATION OF AUTHORISATIONS

10.1 Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed. Authorisations last for:

a) 72 hours if granted or renewed orally beginning with the time of the grant or last renewal, or

b) 12 months from the date of the written grant for the conduct or use of a source

c) three months from the date of grant or latest renewal for directed surveillance

d) one month from the date of written notice or authorisation for communications data, or earlier if cancelled under Section 23(8) of the Act.

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

10.2 Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue and stipulate the frequency of those reviews. The results of a review should be recorded on the central record of authorisations. Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

Any proposed change to the nature of the covert human intelligence source shall be brought to the attention of the Authorising Officer.

Standard review forms for directed surveillance and CHIS are attached at Appendices 4 & 5 and an audit of cases should be periodically undertaken.

10.3 Renewals

Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations

Authorisations can be renewed in writing shortly before the maximum period has expired. An authorisation cannot be renewed after it has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The renewal will begin on the day when the authorisation would have expired.

The Authorising Officer who granted or last renewed the authorisation must cancel it if he is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

Standard renewal forms for the authorisation of directed surveillance and CHIS are contained within the RIPA folder held by Authorising Officers.

Authorisations may be renewed on more than one occasion.

10.4 Cancellations

An Authorising Officer shall cancel a notice or authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the authorising officer who issued it.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

Standard cancellation forms for communications data is attached at Appendix 3, cancellation forms for directed surveillance and CHIS are attached at Appendix 4 & 5.

11 RECORDS

The Council must keep a detailed central record of all authorisations, reviews, renewals, cancellations and rejections in departments and a central register of all such forms will be maintained by the Senior Officer: Democratic and Licensing.

In relation to communications data, the designated SpoC will retain the forms and the Senior Officer: Democratic and Licensing will have access to such forms as and when required.

11.1 Central record of all Authorisations

The Senior Officer: Democratic and Licensing shall hold and monitor a centrally retrievable record of all authorisations. The Authorising Officer must notify and forward to the Senior Officer: Democratic and Licensing whenever a notice or authorisation is granted, renewed or cancelled to ensure that the records are regularly updated. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners. These records will be retained for a period of at least three years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

11.2 Central record of Authorisations and Notices

Authorising Officers must forward details of each form to the Senior Officer: Democratic and Licensing for the central record, within 1 week of the authorisation, review, renewal, cancellation or rejection. The Administration Officer will monitor the same and give appropriate guidance, from time to time, or amend this document as necessary. The record shall contain the following information:

a) the type of authorisation or notice
b) the date the authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the unique reference number (URN) of the investigation or operation;
e) the title of the investigation or operation, including a brief description and names of subjects, if known;
f) whether the urgency provisions were used, and if so why;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
h) whether the investigation or operation is likely to result in obtaining confidential information;
i) the date the authorisation or notice was cancelled.

11.3 Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and a copy of the authorisation or notice 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 or notice;
e) a copy of any renewal of an authorisation or notice, 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.
g) the unique reference number for the authorisation (URN)

Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

11.4 Other Record of Covert Human Intelligence Sources

Proper records must be kept of the authorisation and use of a source. An Authorising Officer must not grant an authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source.

The records shall contain the following information:

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the Council;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source;

  i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare

  ii. have a general oversight of the use made of the source (not to be the person identified in (h)(i))

  iii. have responsibility for maintaining a record of the use made of the source

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by the conduct or use of the source;

(m) any dissemination of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

12 RETENTION AND DESTRUCTION

12.1 Material obtained from properly authorised surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a source or the obtaining or disclosure of communications data. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

12.2 Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

13 CONSEQUENCES OF IGNORING RIPA

13.1 RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then **it shall be lawful for all purposes.**

Where there is interference with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under RIPA may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining or disclosure of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

14 SCRUTINY OF INVESTIGATORY BODIES

14.1 The Office or Surveillance Commissioners (OSC) has been established under RIPA to facilitate independent scrutiny of the use of RIPA powers by the investigatory bodies that are subject to it. The Commissioners will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at www.surveillancecommissioners.gov.uk

14.2 There is also a statutory complaints system welcomed by the Council. The Investigatory Powers Tribunal has been established under RIPA to deal with complaints from members of the public about the use or conduct by public authorities of these powers. The Tribunal is separate from the OSC. The Council welcomes this external scrutiny. It expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

IF IN DOUBT ADVICE MUST BE SOUGHT FROM
CHIEF EXECUTIVE OR THE Senior Officer: Democratic and Licensing

APPENDIX 1

LIST OF RIPA AUTHORISED OFFICERS

As of 7 March 2013, the following officers may grant authorisations:

Theo Leijser	Chief Executive
Richard Burraston	Senior Manager: Democratic and Corporate
Susan Pritchard	Senior Officer: Democratic and Licensing

APPENDIX 2

PROCESS MAP FOR ACCESSING COMMUNICATIONS DATA