Public Document Pack

South Hams District Council

Please reply to: Darryl White
Service: Strategy & Commissioning
Direct Dial: (01803) 861247
E-mail address: Darryl.White@swdevon.gov.uk
Date:

Dear Councillor

SOUTH HAMS AUDIT COMMITTEE - THURSDAY, 4TH FEBRUARY, 2021

I refer to the agenda for the above meeting and attach papers in connection with the following item(s).

Agenda No Item 9 –Appendix C

9. **Regulation of Investigatory Powers Act 2000 (RIPA) Update (Pages 1 - 36)**

Yours sincerely

Darryl White
Senior Specialist – Democratic Services

Encs

This page is intentionally left blank

SOUTH HAMS DISTICT Council
And
WEST DEVON BOROUGH COUNCIL

Regulation of Investigatory Powers Act 2000
Joint Policy

Contents

Introduction

Overview

The Regulation of Investigatory Powers Act 2000 (RIPA) means that formal authorisation from a senior officer must be obtained before carrying out certain surveillance, monitoring and other evidence-gathering activities. The Council may not carry out any other types of surveillance at all.

It is important to remember that RIPA must always be complied with, regardless of whether the information obtained is to be used as evidence in court proceedings. Failure to comply with RIPA doesn't just mean that the evidence cannot be used in court; it means that the whole procedure is illegal and that the officers concerned do not benefit from the above protection.

This Policy applies to South Hams District Council and West Devon Borough Council.

What is this document for and why is it needed?

The Councils' are allowed and required to carry out investigations in relation to their duties. Such investigations may require surveillance or information gathering of a covert nature.

Article 8 of the European Convention on Human Rights provides:

- Article 8.1: Everyone has the right to respect for his private and family life, his home and his correspondence.

- Article 8.2: There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others.

This right is not absolute, it is a qualified right. This means that in certain circumstances the Council *may* interfere with the right if the interference is:

- in accordance with the law
- necessary, and
- proportionate

Covert Surveillance and information gathering may constitute an interference with the right to respect for private and family life. To ensure that such an action is not unlawful under the Human Rights Act 1998, the Council needs to meet the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA).

In simple terms, RIPA requires the Council to have in place procedures to ensure that when required, surveillance is seen as necessary and is properly authorised. Surveillance is usually a last resort that an investigator will use to prove or disprove an allegation. RIPA sets out a statutory mechanism for authorising covert surveillance and the use of covert human intelligence sources (see below). RIPA seeks to ensure that any interference with

an individual's rights under Article 8 is necessary and proportionate and that, therefore, there is a balance between public interest and an individual's human rights. Covert surveillance will only be undertaken where there is no reasonable and effective alternative means of achieving the desired objective.

What is meant by <u>necessary?</u>

It is essential to consider whether an investigation requiring surveillance or information gathering can be done overtly rather than covertly. What would the result be if you carried out the investigation overtly?

If an investigation can be reasonably carried out by any means other than by using covert surveillance, then the use of covert surveillance is not necessary.

It must then be considered whether it is necessary to conduct covert surveillance or use covert human intelligence sources in the circumstances of the particular case for the **purpose of preventing or detecting crime where the offence is punishable by imprisonment of a term of six months or more.**

What is meant by <u>proportionate?</u>

This is an important concept, and it means that any interference with a person's rights must be proportionate to the intended objective. The action must be aimed at pursuing a legitimate aim. Interference will not be justified if the means used to achieve the aim are excessive in all the circumstances.

The use of surveillance must be designed to do no more than meet the objective in question; it must not be unfair or arbitrary, and the impact on the individual (or group of people) concerned must not be too severe. In deciding whether the use or action is proportionate, the risk of intrusion into the privacy of persons other than those who are the object of the investigation must be considered, and the measures proposed to minimise such intrusion must be properly assessed. You must be satisfied that, on balance, the principle of the subject's right to privacy is outweighed by the purpose of the investigation. Clearly, the more serious the matter being investigated, the more likely that surveillance will be proportionate.

The proportionality test will also require you to consider whether there are any other appropriate means of obtaining the information and whether there is a risk of collateral intrusion. The least intrusive method will be proportionate. Some of the things you may also wish to consider in terms of proportionality are whether covert surveillance is the only option, what other options have been considered, the intended length of the investigation, the number of officers to be deployed in the investigation.

The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

<u>What is covered by the Regulation of Investigatory Powers Act 2000?</u>

The main purpose of the Regulation of Investigatory Powers Act 2000 is to ensure that the relevant investigatory powers are used in accordance with human rights. The Act sets out

these powers in more detail. Part II of the Act sets out the powers available to local authorities.

The Council is able to carry out investigations using covert surveillance and/or by using a covert human intelligence source under RIPA following the formal authorisation procedures and codes of practice as set out in this document. RIPA applies to the Council's core functions. Please ask the RIPA Co-ordinating Officer for advice if you are unsure as to whether RIPA will apply.

RIPA not only covers the surveillance of members of the public but would also cover the observation of staff and members as part of an internal investigation.

Do we need to follow these rules?

Although RIPA does not impose a requirement for local authorities to comply with it, it is essential for the Council to do so to ensure that:

- it is less vulnerable to a challenge under the Human Rights Act and
- any material gathered is admissible by the civil and criminal courts.

Following the requirements of RIPA and acting in accordance with this Policy, will therefore protect the Council against potential challenges to its decisions and procedures. Not following the procedures specified in this document could also lead to a complaint of maladministration or a complaint to the independent Tribunal set up under RIPA, details of which are to be found at the end of this document.

What is the relevant legislation?

- The Regulation of Investigatory Powers Act 2000
- The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
- Protection of Freedom Act 2012
- Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500

Authorisation may only be granted if it is necessary for the reason permitted by RIPA. For local authorities the only statutory reason is **for the purposes of preventing or detecting a criminal offence where that offence is punishable (whether on summary or indictment) by a minimum term of at least 12 months imprisonment**.

These penalties only apply to the authorisation of *directed surveillance* and not CHIS

This means that directed surveillance cannot be used for minor offences.

What is the Council's Policy on RIPA?

This document is the Council's policy on RIPA. As such, it should be adhered to unless it is in conflict with either of the Government Codes of Practice which have been made under RIPA. The Codes of Practice are admissible as evidence in court and **must** be complied with.

Copies of the Codes of Practice are available on the Home Office site: https://www.gov.uk/government/collections/ripa-codeswww.homeoffice.gov.uk. These are:

- Covert Surveillance Code Of Practice
- Covert Human Intelligence Sources Code Of Practice

When will this document be reviewed?

This document shall be subject to review once a year. An earlier review may take place should circumstances in the law so require it. Minor amendments may be made from time to time.

Who is responsible for reviewing and monitoring this document and the use of RIPA?

West Devon Borough Council's **Overview and Scrutiny Committee** and South Hams District Council's **Corporate Performance & Scrutiny Panel** are responsible for the overview of the RIPA policy and the Councils' use of RIPA. The Committees will not be involved in making decisions on specific authorisations.

The RIPA Co-ordinating Officer is responsible for;

1. Training and awareness across the Councils
2. Oversight of Authorisations
3. Maintaining and storing records including a retrievable Central Register of authorisations
4. Annual reports to the relevant scrutiny committees
5. Updates and implementation of the RIPA Policy
6. Quarterly reports to the Community Safety Committee (do we have one of these?)

How do I find out more?

General guidance on RIPA may be found on the Home Office site: https://www.gov.uk/government/collections/ripa-codeshttp://www.homeoffice.gov.uk/

Please contact the Council's Legal Section if you require any further advice on RIPA, this document or any of the related legislative provisions.

For the Benefits Section – further guidance may be found in the DWP Circulars.

Surveillance

What is Surveillance?

"Surveillance" includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications
- recording anything mentioned above in the course of authorised surveillance
- surveillance, by or with, the assistance of appropriate surveillance device(s)
- the interception of a communication in the course of its transmission by means of a postal service or telecommunication system if it is one sent by, or intended for, a person who has consented to the interception of the communication.

Surveillance can be overt or covert.

Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly.

General observations made by officers in the course of their duties constitutes overt surveillance.

Warning the person about the surveillance (preferably in writing) constitutes overt surveillance. Consideration should be given to how long the warning should last. This must be a reasonable length of time (three months may be appropriate in many cases), but each case must be assessed as to what is reasonable having regard to the circumstances. Whatever period is chosen, this **must** be set out in the written warning. At the expiry of the period, further written warning should be given otherwise the surveillance will become covert.

Overt surveillance does not require authorisation under RIPA.

Covert Surveillance

"Covert Surveillance" means surveillance which 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.

Covert surveillance does require authorisation under RIPA.

What are the different types of covert surveillance?

RIPA regulates two types of covert surveillance:

- Directed Surveillance, and
- Intrusive Surveillance;

RIPA also regulates the use of Covert Human Intelligence Sources.

Directed Surveillance

Directed surveillance is defined as surveillance which is:

- covert,
- not intrusive (see definition below)
- undertaken for the purposes of a specific investigation or specific operation;
- carried out in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is the target of the investigation or operation); and
- undertaken in a planned manner, and not as an immediate response to events or circumstances.

Intrusive surveillance

Intrusive surveillance is surveillance of any activities on any residential premises or in any private vehicle by a person (other than a Covert Human Intelligence Source) on those premises or in that vehicle or is carried out by means of a surveillance device on the premises or in the vehicle or which provides information of the same quality and details as if it was on the premises or in the vehicle

However, directed surveillance authorisation may be granted for parts of residential premises, such as gardens or driveways which can be observed from the public highway. Further guidance on this point may be obtained from the Council's Legal Section.

It is important to get this right because:

COUNCIL OFFICERS CANNOT CARRY OUT INTRUSIVE SURVEILLANCE

Covert Human Intelligence Sources (CHIS)

The term Covert Human Intelligence Sources is used to describe people who are more commonly known as informants or officers working "undercover". Throughout this document these people are referred to as "Sources"

This does not include members of the public who volunteer information to the Council as part of their normal civic duties or to contact numbers set up to receive information.

A person is a Source if he/she:

- establishes or maintains a covert personal or other relationship for the purposes of:
    - obtaining information; or
    - providing access to information to another person; or
- discloses information obtained by the use or existence of that covert relationship

RIPA authorisation is required for using a Source.

There are special rules for using juvenile or vulnerable persons as sources, and only the Director (HoPS) or in his/her absence the appointed deputy can authorise such surveillance. Further advice should be sought from the Council's Legal Section in such cases.

Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

More information on Juvenile CHIS can be found in the code here https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

Interception of Communications

Local authorities can carry out interception of communications in a restricted number of circumstances.

These are:

In the course of normal business practice

The Councils are permitted without authorisation under RIPA to lawfully intercept its employees' e-mail or telephone communications and monitor their internet access for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems.

The Councils' policies on use of the internet and e-mail are set out on the intranet site under Policies and Procedures/ICT policies.

The Council also has regard to the Employment Practices Data Protection Code – Part 3: Monitoring at Work produced by the Information Commissioner. A copy of this code and its supplementary guidance can be found at: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf~~www.ico.org.uk~~

Interception with the consent of both parties.

Such interception does not require RIPA uthorization, but should be properly recorded.

Interception with the consent of only one of the parties.

Such interception would require RIPA authorisation because it would fall within the definition of surveillance (either directed or using a Source). The main type of interception envisaged here is the recording of telephone calls where either the caller or the receiver has given consent to the recording.

Where as part of an already authorised Directed Surveillance or use of a Source a telephone conversation is to be recorded by the Officer or the Source then no special or additional authorisation is required.

Interception without the consent of either of the parties

The recording of telephone calls between two parties when neither party is aware of the recording **CANNOT BE UNDERTAKEN**, except under a Warrant granted by the Secretary of State under Part 1 of RIPA. Such warrants are only granted by the Secretary of State and it is not envisaged that such activity would fall within the remit of local authority investigations.

.

Procedures

What is the procedure for obtaining authorisation under RIPA?

Directed surveillance and the use of a Source can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

All directed surveillance and use of a Source operations shall be:

- Applied for in writing or verbally in cases of urgency
- Approved
- Monitored
- Renewed when necessary
- Cease when no longer authorised

All the above actions will be carried out in accordance with this document and the relevant Codes of Practice and will be recorded on the Standard Forms listed below:

The Standard Forms are available from the Home Office web-site https://www.gov.uk/government/collections/ripa-forms--2~~www.homeoffice.gov.uk~~

Directed Surveillance

- Application for directed surveillance authorisation
- Review of directed surveillance authorisation
- Application for cancellation of directed surveillance authorisation
- Application for renewal of directed surveillance authorisation

Use of a Source

- Application for conduct-use of a CHIS authorisation
- Review of use of a CHIS authorisation:
- Application for renewal of use of a CHIS authorisation
- Application for cancellation of conduct-use of a CHIS authorisation

Copies of all these documents will be retained and kept on the investigation file as part of the evidence to show that the information gained by directed surveillance or the use of a Source has been obtained legally.

This document provides guidance on the Procedures required to be undertaken by the Investigating Officer and the Authorising Officer for the different stages specified above.

• The Senior Responsible Officer's Duties

Who is the Senior Responsible Officer?

The Councils' Senior Responsible Officer is listed in the annex to this document.

What are my duties?

In accordance with the recommendations of the Codes of Practice, you are responsible for the following areas:-

- the integrity of the process in place within the Council for the management of Covert Human Intelligence Sources and Directed Surveillance
- compliance with Part II of RIPA and the Codes of Practice
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors
- engagement with the OSC inspectors when they conduct their inspections
- oversight of the implementation of any post-inspection action plan approved by the relevant oversight Commissioner
- ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports by the Office of the Surveillance Commissioner

- **The Investigating Officer's Duties under RIPA.**

The Application

The application for authorisation is the responsibility of the Investigating Officer

What do I need to do?

You will need to consider:

- Whether covert surveillance is needed
- Whether directed surveillance or use of a Source is needed
- Whether directed surveillance or use of a Source is necessary for statutory reasons
- Whether directed surveillance or use of a Source is proportionate
- The risk of collateral intrusion
- Safety and welfare arrangements (use of Source only)

These are discussed in more detail below.

What do I need to consider?

- **Consideration: Whether covert surveillance is needed**

Consideration must be given as to whether covert surveillance is needed. You are advised to discuss the need to undertake directed surveillance or the use of a Source with your line manager before seeking authorisation. All options for the use of overt means **must** be fully explored. Remember: if the investigation can be carried out by overt means, then covert surveillance is not necessary.

- **Consideration: Whether directed surveillance or use of a Source is needed**

You must establish which type of "surveillance" is required for the investigation or operation having regard to the guidance contained in this document. The type of surveillance you require affects which application forms you need to complete. Additional considerations are needed for using a Source. Further detail is found below. Combined authorisations for both directed surveillance and the use of a Source may be applied for where appropriate.

- **Consideration: Whether directed surveillance or use of a Source is necessary for the statutory reason**

Authorisation may only be granted if it is necessary for the reason permitted by RIPA. For local authorities the only statutory reason is **for the purposes of preventing or detecting a criminal offence where that offence is punishable (whether on summary or indictment) by a minimum term of at least ~~12~~ 6 months imprisonment**.

This means that directed surveillance cannot be used for minor offences.

You must set out this ground in your application form and provide details of the reasons why it is necessary to use covert surveillance.

- **Consideration: Whether directed surveillance or use of a Source is proportionate**

You must consider why it is proportionate to use covert methods to collect evidence. Please see the definitions set out on page 2 “what is proportionate?” Remember, the use of covert methods must do no more than meet your objective. The proportionality test will also require you to consider whether there are any other appropriate means of obtaining the information and whether there is a risk of collateral intrusion (see consideration below). The least intrusive method will be proportionate. The following aspects of proportionality must be considered and evidenced:-

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result
- evidencing, as far as reasonably practicable, what other methods have been considered and why these were not implemented.

- **Consideration: The risk of collateral intrusion**

Collateral intrusion is the risk of intrusion into the privacy of persons other than the target. You are required to assess the risk of collateral intrusion. Details of any potential collateral intrusion should be specified. Measures must be taken wherever practicable to avoid or minimise collateral intrusion and a plan should be included in your application specifying how the potential for collateral intrusions will be minimised. You should give as much detail as possible, insufficient information may lead to the rejection of the application.

- **Consideration: Surveillance from private premises**

It is preferable for surveillance to be carried out from a public place, such as a public highway. However, there may be circumstances where private premises may be required for the carrying out of surveillance. In which case, it is essential that you obtain the consent of the owner and/or occupier of the premises prior to authorisation being sought. You should seek further guidance from the Council’s Legal Section on this point.

- **Consideration: safety and welfare arrangements – use of a Source**

You must provide a risk assessment as to the likely risks to be faced by an officer or other person both during the conduct of the investigation and after the cancellation of the authorisation. Details must also be included setting out the arrangements for the safety of the Source, this should include:

- the name of the Officer who has day to day responsibility for:
    - Dealing with the Source
    - Directing the day to day activities of the Source

- Recording the information supplied by the Source
- The Source's security and welfare

- The name of the Officer responsible for recording and monitoring the use made of the Source
- Arrangements for ensuring the security of the records which identify the Source
- Records relating to the Source meet the requirements of the Statutory Instrument: The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000 No. 2725) – please see either the Home Office website: www.homeoffice.gov.uk or the Office of Public Sector Information website: www.opsi.gov.uk

How do I apply?

All applications must be made in writing on the standard forms as set out in this document. The relevant forms are:

- An application for directed surveillance authorisation, and/or
- An application for use of a Source

The considerations set out above, form part of the application form.

The application form must be fully completed and passed to the Authorising Officer. The annex to this document contains details of the Council's Authorising Officers.

NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.

What if authorisation is urgent?

The 2012 Home Office Guidance states that in most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. Therefore local councils may need to work with the police if faced with an emergency.

NB. Urgent authorisation may not be necessary if, under section 26(2) of the Act, an officer suddenly sees something relevant to his duties and takes an immediate note, observation of follow-up activity (within reason).

Monitoring

How long will an authorisation last for?

The authorisation for Directed Surveillance will last for **three months** from the date of authorisation unless renewed.

The authorisation for use of a Source will last for **12 months** from the date of authorisation (i.e. date of Magistrates' Order) unless renewed. The authorisation period for a juvenile Source is 1 month less 1 day.

Review dates for the authorisation will be set by the Authorising Officer.

I now have my authority for surveillance, is there anything else I should be aware of?

It will be the responsibility of the Investigating Officer to ensure that any Directed Surveillance or use of a Source is only undertaken under an appropriate and valid authorisation.

During the surveillance, you should ensure:

- Surveillance is carried out in accordance with the approval
- Collateral intrusion is minimised as far as possible
- Intrusive surveillance is not carried out
- All information obtained is recorded contemporaneously or as soon as possible thereafter

During the use of a Source, you should also ensure:

- That the source is aware that:
    - Only the tasks authorised are carried out
    - Third party collateral intrusion is minimised as far as possible
    - Intrusive surveillance is not carried out
    - Entrapment is not committed
    - They must regularly report to you

You should also be mindful of the date when authorisations and renewals will cease to have effect. Please see the notes on Renewals and Cancellation below.

What do I do if circumstances change during the investigation?

You must inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation or if there is another change in circumstances usually brought about by unforeseen action.

When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised (for minor amendments only) or whether it should be cancelled and a new authorisation obtained. The relevant forms should be used.

Particular care should be taken when using a Source to ensure that authorisation is sufficient. It is difficult to predict what might occur each time a meeting with a Source takes place. If unforeseen action takes place, the occurrence should be recorded as soon as possible after the event and the sufficiency of the authorisation must be considered.

You must bring to the attention of the Authorising Officer any concerns about the personal circumstances of the Source in relation to: the validity of the risk assessment; the conduct of the source; the safety and welfare of the Source.

Renewals

Why are renewals important?

Once the authorisation expires, surveillance must cease unless a renewal has been applied for and approved. Renewals must be authorised prior to the expiry of the original authorisation but will run from the date and time of expiry of the original authorisation.

What should I do?

If it appears that the directed surveillance or use of a Source is needed beyond the authorisation date, you must seek a renewal of the authorisation.

You must consider whether covert methods are still necessary and proportionate.

An application for renewal for either Directed Surveillance and/or use of Source should be made on the relevant form and passed to the Authorising Officer for consideration.

Authorisation for renewal may be sought verbally, but only in exceptional circumstances.

NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.

Cancellations

Why are cancellations important?

All authorisations, including renewals, must be cancelled if the reason why Directed Surveillance or use of a Source was required no longer exists or is no longer proportionate. This will occur in most instances when the purpose for which surveillance was required has been achieved and officers must be mindful of the need to cancel any authorisation which has been issued. A cancellation should be issued at the expiry date if not before.

How do I cancel an authorisation?

To cancel an authorisation, you should complete the Cancellation of Authorisation form and submit it to the Authorising Officer for endorsement.

Authorising Officer Responsibilities under RIPA

The Approval

Who are the Authorising Officers?

The Council's Authorising Officers are listed in the annex to this document.

If the investigation may involve the acquisition of confidential or religious material, or require an authorisation for using juveniles or vulnerable persons as sources, the Authorising Officer is, by law, the Head of Paid Service (or in his/her absence the appointed deputy).

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. If this is the case, the application form for authorisation should be noted to this effect.

NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.

What are my responsibilities?

Responsibility for authorising the carrying out of directed surveillance or using a Source rests with the Authorising Officer and requires the personal authority of the Authorising Officer.

You must be satisfied that a defensible case can be made for surveillance. Authorisation is a safeguard against the abuse of power by public authorities. Full consideration of necessity and proportionality will make the action less vulnerable to challenge under the Human Rights Act 1998.

What do I need to consider?

You are required to consider the application for authorisation in relation to the following:

Consideration: Is the directed surveillance or use of a Source necessary?

Firstly, you must consider whether it is necessary to carry out the investigation by covert methods. This is an important consideration and must be recorded on the form.
Please see "what is meant by necessary?" on Pages 1 and 2 of the Policy.

Secondly, as authorisation may only be granted if it is necessary for the reason permitted by RIPA. You should consider, having regard to the outline of the case provided by the Investigating Officer, whether authorisation is necessary for the purposes of preventing and detecting crime or of preventing disorder

Consideration: Is the directed surveillance or use of a Source proportionate?

This involves balancing the intrusiveness of the activity on the target and others who may be affected by it (see "consideration: risk of collateral intrusion" below) against the need for the activity in operational terms. Please refer to "what is proportionate?" on page 2 of this Policy.

Consideration: The risk of collateral intrusion

You must take into account the risk of interfering with the privacy of persons other than the target (collateral intrusion). Full details of potential collateral intrusion and the steps to be taken to minimise such intrusion must be included in the form. If there are insufficient details further information should be sought. Collateral intrusion forms part of the proportionality test and is therefore very important. Remember: the least intrusive method should be chosen otherwise the surveillance activity will not be proportionate.

Consideration: confidential material

In cases where through the use of directed surveillance or the use of a Source it is likely that knowledge of confidential information will be acquired, authorisation may only be granted by the Chief Executive.

Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

Authorisation involving the acquisition of confidential information should only be given in exceptional and compelling circumstances having full regard to the proportionality issues involved.

Further details about the type of information covered under this category are to be found in the Chapter 3 of the relevant Code of Practice. Further advice may be sought from the Council's Legal Section.

Consideration: Safety and welfare arrangements of a Source

When authorising the conduct or use of a Source, you must be satisfied:

- That the conduct and/or use of the Source is proportionate to what is sought to be achieved;
- That arrangements exist for the management and oversight of the Source, particularly the health and safety of the Source including:
    - Identifying the person who will have day to day responsibility for dealing with the Source
    - Security and welfare arrangements of the Source both during and after the investigation/operation.
    - Monitoring and recording the information supplied by the Source
    - Ensuring records disclosing the identity of the Source will not be made available to persons except where there is a need for access to them

- Records relating to the Source meet the requirements of the Statutory Instrument: The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000 No. 2725) – please see either the Home Office website: https://www.legislation.gov.uk/uksi/2007/2196/contents/made~~www.homeoffice.gov.uk~~ or the Office of Public Sector Information website: www.opsi.gov.uk

Consideration: local community

You should consider whether there any particular sensitivities in the local community where surveillance will be taking place.

Having taken all these factors into consideration, you may either approve the application or refuse it.

What do I do if I have refused the application?

You must complete the form and give your reasons for refusal. Then follow the procedures below ("I have completed the form what do I do with it?")

What do I do if I have approved the application?

You need to follow the rest of the procedure set out below.

Regular review should be undertaken to assess the need for surveillance or use of a Source to continue and whether it is still proportionate. Where the surveillance or use of a Source provides access to confidential information or involves collateral intrusion, review should be more frequent.

You will therefore need to consider a Review Date(s). Both types of authorisation require you to specify a date when the authorisation should be reviewed (the Review Date) and the frequency of the review thereafter. This must be stated on the form.

What do I do if the authorisation is urgent?

The 2012 Home Office Guidance states that in most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. Therefore local councils may need to work with the police if faced with an emergency. NB. Urgent authorisation may not be necessary if, under section 26(2) of the Act, an officer suddenly sees something relevant to his duties and takes an immediate note, observation of follow-up activity (within reason).

What do I do with the completed form?

You must send the completed application form(s) to the RIPA Co-ordinating Officer as soon as you are able. This includes any forms in which you have refused authorisation. You should retain a copy of the form and send a further copy to the relevant Investigating Officer for retention on the investigation file.

Monitoring

How long will an authorisation last for?

The authorisation for **Directed Surveillance** will last for **three months** from the date of authorisation unless renewed.

The authorisation for use of a **Source** will last for **12 months** from the date of authorisation unless renewed.

It is important to set a review date which gives the opportunity to cancel if the authorisation is no longer required. If the surveillance is still required, set another review date (see below)

I have now given the authority for surveillance, what should I do next?

After authorisation the Authorising Officer is responsible for continuing to oversee the progress of the investigation. You must ensure that whatever was authorised does actually happen, and that actions do not exceed the boundaries of the authorisation.

Progress of the investigation or operation should be reviewed in accordance with the review dates set by the authorisation using the relevant review form. In any case, as soon as the investigation or operation objectives have been achieved the authority should be cancelled.

You will regularly monitor the surveillance to ensure:

- Surveillance is being carried out in accordance with the authority given
- There is still a need for the approved surveillance or use of the Source
- The surveillance is achieving the intended results
- The risks of collateral intrusion are still minimal
- The risks associated with the surveillance or use of the Source are within an acceptable level
- The security and/or welfare of the Source has not been jeopardised. You must consider any concerns raised by the Investigating Officer relating to the personal circumstances of the Source.

You should record the outcome of such monitoring and take whatever action is appropriate.

Renewals

Why are renewals important?

Once the authorisation expires, surveillance must cease unless a renewal has been applied for and approved.

NB. All authorisations and renewals must have the prior approval of the Magistrates' before they take effect.

What are my responsibilities in respect of renewals?

You may renew an authorisation before it expires if it is necessary for the authorisation to continue for the purpose for which it was given.

You must consider the application for renewal in relation to the original purpose for which authorisation was granted, taking into account any change in circumstances. You should be satisfied that:

- There is a need to renew the authorisation (applying the test of necessity)
- That such a renewal is likely to contribute to the investigation or operation (it is proportionate to the aim)
- That the information could not be reasonably obtained by other less intrusive means.
- The risk of collateral intrusion is minimal – you should consider what collateral intrusion has occurred
- The risks associated with the use of a Source have not increased beyond an acceptable level

The outcome of a consideration for renewal may lead to:

- Approval
- A new application
- Refusal

Approval

If you decide to approve a renewal you will need to provide details of why in your opinion you believe the renewal is justified, and state the date and time when the renewed authorisation will commence and expire on the application form.

The maximum time that renewal of authorisation can be approved for, is three months at a time for directed surveillance and 12 months for the use of a Source, but you may consider shorter periods if this is more appropriate to the circumstances.

You should also set Review Dates and continue to monitor the progress of the investigation or operation.

A new application for authorisation

If the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then the outstanding authorisation should be cancelled and new authorisation sought by way of a new application. You will need to note the refusal to renew the application on the renewal form setting out the reasons for your decision. You will also need to follow the procedures for cancellation see below and advise the Investigating Officer to seek new authorisation.

Refusal

If in your opinion surveillance is no longer required, or justified, or proportionate, the renewal should be refused and the authorisation cancelled. See the paragraph on cancellation below. You will need to note on the renewal form your reasons for refusal.

What do I do with the completed form?

You must send the completed renewal form to the RIPA Co-ordinating Officer as soon as you are able. This includes forms where you have refused a renewal. You should retain a copy of the form and send a further copy to the relevant Investigating Officer for retention on the investigation file.

Cancellations

Why are cancellations important?

All authorisations, including renewals, must be cancelled if the reason why directed surveillance or use of a Source was required no longer exists or is no longer proportionate. This will occur in most instances when the purpose for which surveillance was required has been achieved and officers must be mindful of the need to cancel any authorisation which has been issued. A cancellation should be issued at the expiry date if not before.

What are my responsibilities in respect of cancellations?

The responsibility to ensure that authorisations are cancelled rests with the Authorising Officer. If you think cancellation should have been applied for, then you should make enquiries of the Investigating Officer as part of your monitoring of the authorisation. On receipt of the cancellation form from the Investigating Officer, you must consider the reasons for cancellation and if acceptable endorse the form.

As soon as the decision is taken that directed surveillance or use of a Source should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject. The date and time when such an instruction was given should be recorded on the cancellation form.

Where necessary the safety and welfare of the Source should continue to be taken into account after the authorisation has been cancelled.

What do I do with the completed form?

You must send the completed renewal form to the RIPA Co-ordinating Officer as soon as you are able. This includes forms where you have refused a renewal. You should retain a copy of the form and send a further copy to the relevant Investigating Officer for retention on the investigation file.

Working with or through other Agencies

What do I do if I want to instruct another organisation to carry out surveillance?

When some other agency has been instructed on behalf of the Council to undertake some action under RIPA, this Document and the forms in it, must be used in the normal way and the agency advised as necessary of the various requirements. They must be made aware explicitly what they are authorised to do.

What do I do if I want to carry out an investigation with another organisation?

It is possible for two public authorities to carry out a joint directed surveillance investigation or use of a Source. It must be decided which of the authorities is to take the lead role. The Authorising Officer from the lead organisation must make the decisions on the necessity and proportionality of the surveillance or use of a Source. The Investigating Officer must make it clear on the application form that it is a joint investigation and provide details of Officers involved from both authorities.

Where joint surveillance is authorised by the lead organisation, it is good practice for the Investigation Officer of the other organisation to advise their Authorising Officer of the surveillance activity. It is important for each organisation's Authorising Officer to be aware of all surveillance activity being undertaken by their own Investigating Officers, regardless of which organisation authorised the activity.

Record-Keeping

What records must I keep?

The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all these forms will be maintained and monitored by the RIPA Coordinating Officer.

In all cases, the relevant department should maintain the following documentation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- The Magistrates' Order
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer.
- A record of the use made of any Source

How long must I keep these records?

The Council will retain records in accordance with the Council's Record Management Policy. Retention of a record will therefore depend on an assessment of the need to retain the record.

How should the records relating to a Source be maintained?

Records kept relating to an investigation or operation using a Source should be maintained in such a way as to preserve the confidentiality of the Source and the information provided by the Source. Regard should be had to the Council's Record Management Policy.

Material obtained from Directed Surveillance and/or use of a Source operations

How should material be handled and stored?

Material, or product, such as: written records (including notebook records); video and audio tape; photographs and negatives; and electronic files, obtained under authorisation for Directed Surveillance or use of a Source investigations or operations should be handled, stored and disseminated according to the following guidance and with regard to the Council's Records Management Policy, which is available on the intranet.

Where material obtained during the course of an investigation may be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with the established disclosure requirements having regard to the Criminal Procedure and Investigations Act 1996 and Civil Procedure Rules.

Where material is obtained which is not related to a criminal or other investigation, or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be assessed for retention or destruction under the Council's Record Management Policy.

Material may be used in investigations other than the one which authorisation was issued for. However, use of such material outside the Local Authority or the Courts should only be considered in exceptional circumstances.

What about confidential material?

This is privileged information from, for example, lawyers, doctors, priests etc. Where such persons are involved, and there is a possibility that you maybe obtaining confidential material, then further additional precautions must be taken. If this is the case, please seek appropriate advice from the Legal Section or from the statutory RIPA Code of Practice.

(Lord Coleville advised that reference only to confidential material is needed, as we are very unlikely to ever use these provisions.)

Complaints

The Regulation of Investigatory Powers Act has established an Independent Tribunal. This Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any cases within its jurisdiction. It also has the power to award compensation.

Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Other actions that could be taken against the Council for failing to meet the requirements of RIPA are civil proceedings under the Human Rights Act 1998 or a complaint to the Ombudsman.

Annex A

AUTHORISING OFFICERS

The following Officers shall be designated Authorising Officers on behalf of West Devon Borough Council and South Hams District Council under the Regulation of Investigatory Powers Act 2000.

CHIEF EXECUTIVE (Head of Paid Service) – Andy Bates
DEPUTY CHIEF EXECUTIVE – Steve Mullineaux
STRATEGIC FINANCE DIRECTOR – Lisa Buckle
DIRECTOR of GOVERNANCE AND ASSURANCE – Drew Powell
DIRECTOR of PLACE & ENTERPRISE – Chris Brook

NB. Only the Chief Executive (Head of Paid Service) or in his/her absence the appointed deputy has the authority to grant authorisation for the acquisition of confidential information or where the authorisation would involve juvenile or vulnerable CHIS.

SENIOR RESPONSIBLE OFFICER

The following Officer shall be designated Senior Responsible Officer on behalf of the Councils' under the Codes of Practice.

~~**CHIEF EXECUTIVE (Head of Paid Service) – Andy Bates**~~ **Director of Governance and Assurance – Drew Powell**

RIPA CO-ORDINATING OFFICER

Legal Specialist and Solicitor – Becky Fowlds

ANNEX B

Guidance on the use of Social Networking Sites for investigations

It is recognised that the use of the internet and, in particular, social networking sites, can provide useful information for South Hams District Council and West Devon Borough Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the council – for example Fraud, Planning Enforcement, Licensing or Environmental Health, but will equally apply to some non-enforcement teams, such as Debt Collection or Housing. The use of the internet and social networking sites may fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy).

Social Networking Sites

There is a fine line between general observation, systematic observation and research and it is unwise to rely on a perception of a person's reasonable expectations or their ability to control their personal data.' The Councils' policy in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below:

 Officers of South Hams and West Devon must not 'friend' individuals on social networks as part of undertaking their roles and should not use their own private social networking accounts to view the social networking accounts of other individuals as part of their professional role

 officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation

 further viewing of open profiles on social networking sites to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate

 officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

The **purpose** of this guidance note is to provide clarity on the Councils' position:

9. It is not possible to provide a definitive list of social networking sites, so this should be taken to mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether accepted as 'friends' or otherwise.

This might include sites such as 'Facebook' and 'LinkedIn'.

9. As the definition of 'private information' under RIPA includes:

   'any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships'

Sites used to advertise goods and services should be included within the definition. Although there is likely to be a reduced expectation of privacy with this type of site, there is still the possibility of obtaining private information which may be subsequently used in any enforcement proceedings.

9. If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile once in order to take an initial view as to whether there is any substance to the allegation or matter being investigated.

4. The initial viewing must be reasonable – for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual's profile or to print out several pages just in case they may reveal something useful.

5. In some cases where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing. However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.

6. Each single viewing of an individual's social networking site must be recorded on the log maintained by Legal Services (RIPA Co-ordinating Officer). This is to enable the reporting of the number of viewings to the Overview & Scrutiny Committee of each Council.

7. If it is considered that there is a need to monitor an individual's social networking site, authorisation must be obtained from an Authorising Officer.

8. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by one of the Councils' Authorising Officers and then approved by a Magistrate.

9. If the offence being investigated falls outside of RIPA (for example if the offence does not carry a custodial sentence of at least 12 months imprisonment or is not a core function of the council) a non-RIPA form must be completed General guidance on RIPA and appropriate forms can be found on the Councils' Intranet and in the main RIPA Policy document.

Annex C

Procedure to be adopted for obtaining the approval of a magistrate

The government guidance for obtaining authorisation from a magistrate for surveillance is contained in full at Annex D.
The relevant form is set out below as Form 1.

FORM 1

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance.
Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.
Local authority:.....
Local authority department:.....
Offence under investigation:.....
Address of premises or identity of subject:.....
.....
.....
.....
.....

Covert technique requested: (tick one and specify details)
Communications Data
Covert Human Intelligence Source
Directed Surveillance

Summary of details
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

refuse to approve the grant or renewal of the authorisation/notice.

refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....
.....
Reasons
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Signed:
Date:
Time:
Full name:
Address of magistrate

Appendix D