Regulation of Investigatory Powers Act 2000

Policy and Procedural Guidance on the Use of Covert Surveillance

Reviewed November 2023

CONTENTS

1.Introduction

The Council has a number of regulatory and enforcement responsibilities. These functions are primarily for the purpose of protecting the wider community from criminal activity and public disorder.

The regulatory and enforcement activity and the responsibility to ensure the safety of the community require the Council to pursue and enforce statutory activity where appropriate which may require the use of investigatory powers.

Article 8 of the Human Rights Act 1998, states that:

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 activity is in accordance with the law the Council should ensure that surveillance is carried out in accordance with the **Regulation of Investigatory Powers Act 2000 (RIPA)** where appropriate.

A person with the authority to authorise directed Surveillance or Covert Human Intelligence Sources may be the Deputy Chief Executives**,** Group Head of Service, Service Manager or equivalent.

RIPA was enacted to provide a lawful procedure for public bodies to carry out covert investigations without the risk of a claim being made under the Human Rights Act 1998, against either the body or the Investigating Officer, by the person subject to such an investigation.

RIPA also provides for oversight by the Investigatory Powers Commissioner's Office (IPCO). IPCO conducts inspections, publishes annual reports, and procedures and guidance.

When making an application for covert surveillance, local authorities must be satisfied that surveillance is both necessary and proportionate.

2. Grounds for Necessity

2.1 Necessity

The **Statutory grounds for necessity** are set out within the legislation. There are several statutory grounds, however the Council may only use RIPA authorisation for one statutory ground detailed in Sec 28(3) and Sec 29(30) of the Regulation of Investigatory Powers Act –

(b) – The purpose of preventing or detecting crime or preventing disorder.

If the proposed conduct is necessary, those involved with the process must make reference to the relevant section within the codes of practice, issued by the Home Office which can be accessed at the link below.

Both applicant and authorising officer must articulate in their own words why the proposed activity is necessary in all of the particular circumstances relating to the case concerned.

Since the implementation of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, **the circumstances in which local authorities may authorise directed surveillance are now restricted** to the investigation of offences which are punishable by a maximum term of at least six month's imprisonment or are related to the underage sale of alcohol and tobacco or nicotine inhaling products.

2.2 Proportionality

If the proposed conduct is proportionate, those involved with the process must make reference to the relevant section within the codes of practice.

Both applicant and authorising officer must articulate in their own words why the proposed activity is proportionate in all of the particular circumstances relating to the case concerned,

Any consideration of proportionality should contain a consideration of the three elements:

(a) That the proposed covert surveillance is proportional to the mischief under investigation.

(b) That it is proportional to the degree of anticipated intrusion on the target and others; and

(c) It is the only option, other overt means having been considered and discounted.

The Codes of Practice are admissible as evidence in court and **must** be complied with. In the event of a trial or hearing this Policy might also be adduced in the court.

Useful link
https://www.gov.uk/government/collections/ripa-codes

3. Terms and Definitions

3.1 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.

3.2 Overt Surveillance

Most of the surveillance done by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases officers will be behaving in the same way as normal members of the public and/or will be going about Council business openly.

A general observation 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 and each case must be assessed as to what is reasonable having regard to the circumstances.)

Overt surveillance does not require authorisation under RIPA.

3.3 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 if other criteria as set out within the codes also apply.

4. 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.

4.1 Directed Surveillance

Directed surveillance is defined as surveillance which is:

- Covert
- Not intrusive
- 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 pre-planned manner, and not as an immediate response to events or circumstances.

If the proposed activity fulfils all of the criteria for directed surveillance, RIPA authorisation is required.

4.2 Intrusive surveillance (**not permitted by the Council**)

Intrusive surveillance is surveillance in any residential premises or in any private vehicle carried out by a person or by means of a surveillance device on the premises or in the vehicle which provides information of the same quality and details as if it was on the premises or in the vehicle.

4.3 Covert Human Intelligence Sources

The term Covert Human Intelligence Sources is used to describe people who are more commonly known as informants or offices working ‘undercover’.

Throughout this document these people are referred to as “CHIS”.

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.

4.4 Definition of CHIS

Under RIPA, a person is a CHIS if:
• they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within Section 26(8)(b) or (c);
• they covertly use such a relationship to obtain information or to provide access to any information to another person; or
• they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is established or maintained for a covert purpose if and only if it 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 the relationship is used or the information is 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 Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 ("the 2013 Relevant Sources Order") further defines a particular type of CHIS as a "Relevant Source". This is a source holding an office, rank or position with the public authorities listed in the Order and Annex B to the Covert Human Intelligence Sources Code issued by the Home Office. Enhanced authorisation arrangements are in place for this type of CHIS as detailed in this Code. Such sources will be referred to as a "Relevant Source" throughout this Code. RIPA authorisation is required for CHIS activity.

If CHIS are to be used there should be a controller who will have overall control of the operation involving the use of the CHIS.

There are particular procedures relating to the conduct and use of CHIS authorisation, together with risk assessment and other procedures. There are also issues relating to the management of the personal details of a CHIS and the information obtained as a result of such activity. **Whilst the Council will make use of CHIS authorisation if appropriate, it is a tactic that must be discussed with the Legal Department.**

There are also special rules for using juveniles or vulnerable persons as CHIS, and only the Chief Executive can authorise such surveillance (or in his absence his nominated deputy).

If the conduct to be authorised may involve the acquisition of confidential or religious material or require an authorisation for using juveniles or vulnerable persons as CHIS, the Authorising Officer is, by law, the Chief Executive (or in his absence the Deputy Chief Executive who has been nominated to act in his place).

Further advice should be sought from the Council's Legal Department in such cases.

5. Authorisation Procedures

Directed Surveillance and the use of a CHIS can only be lawfully carried out if properly authorised and conducted in strict accordance with the terms of the authorisation.

All directed surveillance and use of CHIS shall be:

- Applied for in writing
- Authorised by an appointed Authorising Officer and subsequently by a Justice of the Peace
- Conducted in accordance with the authorisation
- Monitored and reviewed when required and in any case in accordance with reviews set by the Authorising Officer
- Renewed if applicable
- Cancelled as soon as the objective has been achieved or the activity is no longer to be conducted, whichever is sooner

5.1 The Standard Forms

Directed Surveillance

- Application for directed surveillance authorisation
- Application to Magistrates' Court
- Review of directed surveillance authorisation
- Application for cancellation of directed surveillance authorisation
- Application for renewal of directed surveillance authorisation

Use of CHIS

- 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

The Standard Forms are available from the Legal Services office.

6. Applications for Judicial Approval

Sections 37 and 38 of the Protection of Freedoms Act 2012 came into effect on 1 November 2012. This legislation means that a local authority who wishes to authorise the use of directed surveillance, and use of CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace, JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

6.1 Making the Application

The application must be made by the public authority that has granted the authorisation. Following approval by the authorising officer/designated person the first stage of the process is for the local authority to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.

The local authority will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**.

Wherever possible the authorising officer will attend court with the Investigating Officer.

6.2 Decision of the JP

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition, they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

6.3 Outcomes of the Hearing
After the JP has considered the case, there are three conclusions which he/she may reach.

The JP may either:

- **Approve the Grant or renewal of an authorisation or notice** – the grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case.

- **Refuse to approve the grant or renewal of an authorisation or notice** – the RIPA authorisation or notice will not take effect and the local authority may **not** use the technique in that case. Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

- **Refuse to approve the grant or renewal and quash the authorisation or notice** – this applies where a Magistrate's Court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice. The Court must not exercise its power to

quash that authorisation or notice unless the applicant has had at least two business days from the date of the refusal in which to make representations.

Useful Link
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

7. The Senior Responsible Officer's Role

The Council's Senior Responsible Officer is the Group Head of Corporate Governance who is responsible for:

- The integrity of the process in place within the Council for the management of CHIS 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 IPCO inspectors when they conduct their inspections
- Oversight of the implementation of any post-inspection action plan approved by IPCO

7.1 Management of Records

The Senior Responsible Officer is responsible for ensuring a central register of authorisation is maintained.

The register and all associated documents relating to authorisations, reviews, cancellations, or renewals and refused applications should be retained in an auditable format, with each particular authorisation allocated a unique reference number for that particular investigation or activity.

The Senior Responsible Officer is responsible for submitting annual statistics to IPCO in relation to authorisations.

The Senior Responsible Officer is also responsible for communicating to IPCO any unauthorised activity that might come to the attention of the authority. This must be done within five working days. The records, documentation, and associated documentation relating to this unauthorised activity must be retained by the Senior Responsible Officer and disclosed to IPCO upon request, and certainly to an inspector from the IPCO at the commencement of the next scheduled inspection.

Management of the records by the Senior Responsible Officer requires that person to carry out sufficient audit and checking in order to provide for a reasonable level of quality control. Any identified issues should be communicated with the authorising officer and any others concerned in order to ensure review drives improvement in compliance.

8. The RIPA Monitoring Officer's Role

The Council's RIPA Monitoring Officer is the Legal Services Manager, responsible for:

- Maintaining the central register of authorisations and collating the original applications/authorisations, reviews, renewals and cancellations
- Oversight of submitted RIPA documentation

9. The Applicant's Role

The application

You will need to consider:

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 CHIS with your line manager before seeking authorisation. All other options to obtain the information to be obtained by the authorised activity should be considered and used if appropriate.

Whether Directed Surveillance or the use of CHIS is needed

You must establish what type of 'surveillance' is required having regard to the guidance contained in this document. The type of surveillance you require affects which application forms you need to complete.

Whether Directed Surveillance or use of a CHIS is necessary for statutory reasons (identify the particular offence to be prevented or detected or what disorder is to be prevented)

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 and detecting crime or of preventing disorder (and now for certain offences only). You must set out this ground in your application form and provide details of the reasons why it is necessary to use covert surveillance.

Whether Directed Surveillance or use of CHIS is appropriate

You must consider why the activity applied for is proportionate.

The methods must do no more than ensure you 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) and how this can be minimised or managed, or it if is acceptable in the circumstances.

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 is reasonably practicable, what other methods have been considered fully and why these were not implemented.

The risk and amount 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.

Conduct a risk assessment in relation to health and safety of personnel and public (not a statutory requirement under RIPA, but an operational requirement)

This requirement is not in relation to compliance with RIPA. However, it is a fundamental requirement when conducting any activity at work. The risk assessment helps the line manager and the authorising officer to consider the health and safety risks to the personnel and public are identified, and if possible measured and controlled, and only the level of risk to be taken will be that which reflects the benefit to the authority.

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 carrying out the surveillance. In which cases, 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 Department since there are other considerations in relation to management of CPIA Disclosure, and use of the product of the surveillance as evidence.

10. Standard Forms for Making an Application

All applications must be made in writing on the standard forms provided.

The relevant forms are:

- An application for directed surveillance authorisation, and/or
- An application for the use of a CHIS
- An application to a Justice of the Peace

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

10.1 Authorisation Duration

An authorisation for Directed Surveillance will last for three months from the date of authorisation unless renewed. It must be cancelled as soon as it is no longer required.

An authorisation for use of adult CHIS will last for twelve months from the date of authorisation unless renewed.

Review dates for the authorisation will be set by the Authorising Officer. All authorisations must be cancelled as soon as they are no longer required and must not be allowed to expire.

During the course of an investigation, the type and seriousness of offences may change. The option of authorising directed surveillance is dependent on the offence under investigation attracting a sentence of maximum six months imprisonment or more or being related to the underage sale of alcohol and tobacco. Providing the offence under investigation is one which appears on the statute book with at least a maximum six months term of imprisonment or is related to the specific offences listed in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 as amended, concerning the underage sale of alcohol or tobacco, an application will be made. However, if during the investigation, it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

10.2 Conduct of Authorisation

It will be the responsibility of the applicant and persons conducting the authorised activity to ensure that any Directed Surveillance or use of CHIS is only undertaken under an appropriate and valid authorisation.

During the surveillance, you should ensure:

- Surveillance is carried out in accordance with the authorisation
- Collateral intrusion is monitored and minimised as far as possible
- Intrusive surveillance is not carried out
- All information obtained is recorded and managed appropriately and in accordance with the Data Protection Act (subsequently other legislation such as PACE and CPIA are likely to apply to the product of the surveillance).

During the use of CHIS, 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
- Agent Provocateur (Entrapment) is not committed
- They must regularly report to you

You should also be mindful of the date when reviews and renewals are required.

You must inform the Authorising Officer if the authorised activity unexpectedly interferes with the privacy of individuals who are not covered by the authorisation or if there is another change in circumstances usually brought around 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 CHIS to ensure that authorisation is sufficient. It is difficult to predict what might occur each time a meeting with CHIS 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 CHIS in relation to: the validity of the risk assessment; the conduct of the CHIS; the safety and welfare of the CHIS.

Renewals

If it is required, a renewal must be authorised prior to the expiry of the original authorisation. Applications for renewal should be made on the appropriate form shortly before the original authorisation period is due to expire. Officers must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a Magistrate to consider the application). 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. Renewals of an authorisation may be granted more than once, provided the criteria for granting that authorisation are still met. However, if the reason for requiring the authorisation has changed from the purpose for which it was originally granted, then it should be cancelled, and new authorisation sought. The renewal will begin on the day when the original authorisation would otherwise have expired.

Cancellations

All authorisations, including renewals, must be cancelled if the reason why Directed Surveillance or use of CHIS 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.

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

Equipment

Equipment and surveillance logs should be allocated from a central record of equipment, and an audit trail maintained in relation to the equipment and surveillance logs.

Upon cancellation all equipment in use must be removed immediately or else as soon as practicable, since further recordings will amount to unauthorised surveillance.

11. Authorising Officer Responsibilities under RIPA

If the conduct to be authorised may involve the acquisition of confidential or religious material, or require an authorisation for using juveniles or vulnerable persons as CHIS, the Authorising Officer is, by law, the Chief Executive (or in his absence one of the Deputy Chief Executives)

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 together with an explanation as to why this has taken place.

Authorising Officer Responsibilities – Responsibility for authorising the carrying out of direct surveillance or using a CHIS 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 the conduct authorised.

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.

You should refer to both the relevant Codes of Practice when fulfilling your role, and if required seek the guidance of the Legal Department and Senior Responsible Officer on issues that you are uncertain about.

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

Crime Threshold
Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can now

only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are offences which attract a maximum custodial sentence of six months or more or are offences relating to the underage sale of alcohol or tobacco.

Necessity

Firstly, you must consider whether it is **necessary** to carry out the covert activity. This is an important consideration and must be recorded on the form. The Codes of Practice provide guidance in relation to this consideration.

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 applicant, whether authorisation is necessary for the purposes of **preventing or detecting certain crimes only or of preventing disorder**.

Proportionality

This involves balancing the intrusiveness of the activity on the target and others who may be affected by it against the need for the activity in operational terms. The Codes of Practice provide guidance in relation to this consideration.

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. The application form should detail expected collateral intrusion, what has been done to minimise or control it, why the expected level is unavoidable but acceptable in the circumstances, what other investigative methods have been pursued or considered, and why this activity is the chose option.

If equipment is to be used you should enquire with the operative as to its capability and the extent to which it is to be used in order to be able to recognise what might be recorded.

Confidential Material

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

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 relevant Code of Practice. Further advice may be sought from the Council's Legal Department.

Safety and Welfare arrangements of CHIS
When authorising the conduct or use of a CHIS, you must be satisfied:

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

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

Authorisation
Having taken all these factors into consideration, you may either approve the application or refuse it. You can authorise some of the activity applied for, but cannot add and authorise other activity you feel is appropriate. If there is further activity that should be conducted that is not contained within the application, a further application will be required, and then considered upon its merits.

Authorisation Refused
You must complete the form and give your reasons for refusal. Then follow the procedures below.

Authorisation Approved
The applicant or operative responsible for the conduct authorised must be informed exactly what activity has been authorised.

Before the Authorisation can take effect, the local authority must obtain an order approving the Authorisation or a renewal from a JP (a District Judge or Lay Magistrate). If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal as set out in the Authorisation.

Regular reviews should be set and undertaken to assess the continued need for surveillance or use of a CHIS and whether it is still proportionate.

Where the surveillance or use of CHIS provides access to confidential information or involves collateral intrusion, reviews should be more frequent. You will therefore need to consider a relevant appropriate 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.

Authorisation Duration
An authorisation for Directed Surveillance will last for three months from the date of authorisation unless renewed.

An authorisation of use of CHIS will last for twelve months from the date of authorisation unless renewed. Urgent authorisation for either Directed Surveillance or use of CHIS will last seventy-two hours beginning with the time when the authorisation was confirmed by a JP, unless subsequently endorsed by written authorisation.

Authorisation Review
It is important to set a review date which gives the opportunity to review the level of collateral intrusion and the effectiveness of the methods used. Reviews should be more frequent to reflect any particular concerns you might have.

If surveillance is to be continued, set another review date. If the authorisation is to be cancelled, submit the relevant signed cancellation form.

Renewals
Once the authorisation expires, surveillance must cease unless a renewal has been applied for and approved. You may apply for a renewal of an authorisation before it expires if it is necessary for the authorisation to continue for the purpose for which it was given (but a further JP confirmation will still be required).

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 has not altered – you should consider what collateral intrusion has occurred
- The risks associated with the use of CHIS have not increased beyond an acceptable level.

The outcome of a consideration of renewal may lead to:

- Approval
- A new application

- Refusal

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

The maximum time that renewal of authorisation can be approved for, is three months at a time for directed surveillance and twelve months for the use of a CHIS. You should also set appropriate Review Dates.

A new application for authorisation
IF the application circumstances resulting in the original authorisation have changed 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 and advise the applicant 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. You will need to note on the renewal form your reasons for refusal.

Cancellation
All authorisations, including renewals, must be cancelled if the reason why directed surveillance or use of CHIS 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.

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 as part of your monitoring of the authorisation. On receipt of the cancellation form 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 CHIS 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 CHIS should continue to be taken into account after the authorisation has been cancelled.

All equipment should be retrieved and recording ceased.

The product of the authorised activity is your responsibility, not in so much as you personally take possession of it, but you ensure directions and processes are in place to ensure its appropriate management in accordance with Data Protection and other relevant legislation.

Review upon Cancellation
There should be a full review of the usefulness of the authorised activity. This should include what has been achieved and what was not. The review should identify why any objectives were not achieved. This information should be recorded and presented upon inspection by the IPCO Inspector. The information should also be used by all involved in the procedures in order to educate future applications and authorisations.

12. Working with or through other Agencies

When some other agency has been instructed on behalf of the Council to undertake some action under RIPA, the procedures must be applied 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.

They are acting as agents of the Council and must follow the same procedures as Council personnel.

It is possible for two public authorities to carry out a joint directed surveillance investigation or use of CHIS. 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 necessary and proportionality of the surveillance or use of CHIS. This Authorising Officer authorises the activity he or she feels appropriate.

If resources such as personnel or equipment belonging to the other agency within the investigation are to be used, the authorisation must be seen and then the use of the resources authorised by the relevant line manager.

13. Record Keeping

13.1 **Records maintained in the Department**

The Authorising Officer shall maintain the following documentation ideally in one secure and central location. Maintaining copies in different locations is to be avoided and can complicate the application of retention, review and destruction processes. a) a copy of the application and provisional authorisation or notice together with a copy of any order of judicial approval or refusal, as well as 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 judicial approval or refusal and 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 provided by the RIPA Monitoring Officer. 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.

13.2 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 a provisional authorisation for the use or conduct of a source unless they believe 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.

SAFEGUARDS FOR RETENTION, REVEW AND DESTRUCTION OF MATERIAL OBTAINED THROUGH COVERT POWERS

Material obtained in the course of criminal investigations and which may be relevant to the investigation must be recorded and retained in accordance with the Criminal Procedure and Investigations Act 1996. The Council must have in place arrangements for the handling, storage and destruction of material obtained through the use of covert surveillance and compliance with the appropriate data protection requirements must be ensured. The Council's Information Governance Policy, Strategy and Framework must be adhered to. In addition, before any authorisation is approved, advice on the handling, dissemination, copying, storage, security, retention and destruction of covert surveillance material must be sought from the RIPA Monitoring Officer and the ICT Manager, in order to ensure the Council complies with the additional safeguarding obligations contained in the relevant Home Office Codes of Practice. This Policy document shall be kept under review to ensure it is consistent with the Safeguards chapter of the relevant Home Office Code of Practice, as may be amended. There will be a suitable audit trail for the eventual destruction of product, including the means by which an officer(s) will be designated to check this is being carried out as intended. An additional entry in the Central Record may be used as a suitable means to capture this. The Council's Information Governance Policy and Information Asset Register will on review consider a reference to the Safeguards for RIPA/IPA product with a link to the main Corporate Surveillance Policy section for further advice. The Council will ensure that internal safeguard policies for retaining, reviewing and disposing of any relevant data are accurate and up-to-date.

Authorising Officers will through training have an understanding of any data pathways used for RIPA or IPA data. Authorising Officers will familiarise themselves with retention policies and know who will be personally responsible for retention, review and destruction of data shown on the central record. All data obtained under IPA and RIPA will be clearly labelled and stored on secure shared corporate repositories (e.g. Sharepoint as applicable).

All electronic copies of the signed authorisations, will be retained for three years and then disposed of securely, unless it is believed that the records could be relevant to pending or future criminal proceedings, where they must be retained for a suitable further period, commensurate to any subsequent review. The Council will ensure that all material acquired during covert surveillance is held in secure locations, with clear

handling instructions in place when material exchanges hands, and a clear retention, review, destruction (RRD) schedule will be applied to all copies made.

14. Material obtained from Directed Surveillance and/or use of CHIS operations

Material, or product, such as: written records (including notebook records); video and audio recordings; photographs and negatives; and electronic files, obtained under authorisation of Directed Surveillance or use of a CHIS investigations or operations should be handled, stored and disseminated according to the following guidance and with regard to the Council's Data Protection Policy.

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 Data Protection Policy.

Material may be used in investigations other than the one for which authorisation was issued.

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 Data Protection Policy.

Material may be used in investigations other than the one for which authorisation was issued.

Confidential Information

This is privileged information from, for example, lawyers, doctors, priests etc. Where such persons are involved, and there is a possibility that you may be obtaining confidential material, then further additional precautions must be taken. If this is the case, seek appropriate advice from the Legal Department.

15. Social Networking Sites and Internet Sites

Social Networking Sites (SNS) which include but are not limited to Facebook, Instagram, Twitter and TikTok can provide information that will aid an investigation. When using these sites to carry out surveillance it is essential to know how they work and officers should not assume that one service provider works in the same way as another.

In all cases it would be unwise to assume that the content came from an open source or was publically available, even where security settings are low, as the

author would have some reasonable expectation of privacy where access controls are applied.

When conducting any surveillance of social media sites use of an officers personal account is prohibited and advice should be sought from the Communciations Team with regards to setting up a Council account. It may pose a risk to an officers' personal safety when viewing social media profiles from a personal account, due to the potential for a 'digital footprint' to be left and therefore potentially identifying the officer to the account holder.

Where a site is being covertly accessed for monitoring purposes it may be necessary for an authorisation for directed surveillance to be obtained. As part of an investigation, it is possible to take an initial look at an individual's social media activity, however, should there be a need to return to the site this may constitute surveillance. In such circumstances advice should be obtained from the RIPA Co-ordinating Officer before further surveillance is carried out.

When accessing an individuals' social media site, an officer of the Council must never establish or maintain a relationship with that individual without consulting with the SRO, as an authorisation for a CHIS may need to be obtained. See above for full details of what constitutes a CHIS.

The Central Record will contain a register of any Council profiles utilised and a record of their use, where the Council decides to utilise Social Media for the purpose of investigation. The RIPA Monitoring Officer must be involved prior to any social media being utilised for surveillance, to ensure appropriate records are being kept and stored.

Accessing Communications data

Only authorised officers are able to use the NAFN Single Point of Contact service to access communications data. NAFN provides Council officers with access to a secure online system for processing RIPA telecommunications requests. Authorised applicants and designated persons can submit, approve and track applications through one central secure website. NAFN review all applications for legal compliance prior to approval from Swale's designated person. NAFN is subject to inspection by the officers of the Interception Commission to ensure compliance with RIPA.

16. Complaints

The Regulation of Investigatory Powers Act established the Investigatory Powers Tribunal an independent tribunal 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
P O 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

AUTHORISING OFFICER(S)

The following Officer(s), shall be designated Authorising Officers on behalf of the Council under the Regulation of Investigatory Powers Act 2000.

Senior Planning Lawyer
Strategic Planning Manager
Planning Development Manager
Senior Environmental Health Manager
Chief Executive
Deputy Chief Executive

SENIOR RESPONSIBLE OFFICER – Group Head of Corporate Governance