REGULATION OF INVESTIGATORY POWERS ACT POLICY

Contents

Introduction

The Council has a number of regulatory and enforcement responsibilities. These functions are primarily for the purpose of protecting the greater good of the wider community within the jurisdiction of the Council.

The regulatory and enforcement activity, and the responsibility to ensure the safety of the community requires the Council to pursue and enforce statutory activity where appropriate.

The investigations required to fulfil these duties 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 ina 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 rely upon the **Regulation of Investigatory Powers Act 2000 (RIPA)** where appropriate.

The Council is listed as a **'Relevant Public Authority'** within **Statutory Instrument 2010 No. 521. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.**

The Statutory Instrument describes the prescribed office of a person with the authority to authorise directed surveillance or a Covert Human Intelligence Source as **Director, Head of Service, Service Manager or equivalent.**

RIPA sets out a statutory mechanism for authorising covert surveillance and the use of covert human intelligence sources.

RIPA requires the Council to have in place procedures to ensure that RIPA activity is in accordance with the law, compliant with the relevant Codes of Practice.

RIPA also provides for oversight by the Investigatory Powers Commissioners Office (IPCO). The IPCO conduct inspections publish annual reports, and procedures and guidance.

The Council endeavours to ensure the guidance provided by these resources, together with case law and Investigatory Powers Tribunal (IPT) judgements, educate and inform policy and procedure within the Council.

The Council provides training on a regular basis to ensure relevant personnel have adequate skills and knowledge and are updated in relation to current developments.

Grounds for Necessity

Necessary

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(3) of the R~~egulation of I~~~~nvestigatory~~ P~~owers A~~~~ct~~ -

(b) - The purpose of preventing or detecting crime or of preventing disorder

As to if the proposed conduct is necessary, those involved with the process must make reference to the relevant section within the codes of practice~~, and also the OSC Procedures and Guidance 2016 for guidance~~.

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

The lawfulness of the activity relies upon (amongst other issues), necessity.

As a consequence of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, the circumstances in which local authorities may authori~~s~~z~~z~~e directed surveillance is now restricted to the investigation of offences which are punishable by a maximum term of at least six months imprisonment or constitutes an offence under sections 146, 147 or 147a of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1993 (sale of tobacco to children under 18 years old).

Commented [ML1]: This document was withdrawn as was produced by organisation that no longer exists.

Proportionality

As to if the proposed conduct is proportionate, those involved with the process must make reference to the relevant section within the codes of practice~~, and also the OSC Procedures and Guidance 2016 for guidance~~.

Both applicant and authorising officer must articulate in their own words why theproposed 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 lawfulness of the activity relies upon (amongst other issues) proportionality.

Commented [ML2]: This document was withdrawn as was produced by organisation that no longer exists.

RIPA Compliance and Council Policy

Although RIPA does not impose a requirement for the Council to comply with it, it is essential for the Council to do so to ensure that it is less vulnerable to a challengeunder the Human Rights Act and that any material gathered is in accordance with the law.

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.

This document is the Council's policy on RIPA. As such, it should be adhered to unlessit is found to conflict with changes in law, or either of the Codes of Practice which have been made under RIPA.

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.

Policy Review

This policy will be reviewed on an annual basis. Earlier reviews will take place should circumstances such as changes in law, case reviews, or other similar circumstances so require it. Minor adjustment may be made from time to time.

The policy will be presented for review, to Elected Members on an annual basis or earlier if substantial amendment is required.

Terms and Definitions

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

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

Different Types of Covert Surveillance

RIPA regulates two types of covert surveillance:

- Directed Surveillance, and
- Intrusive Surveillance; - **The Council cannot conduct 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)
- undertake 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, then RIPA authorisation is required*.**

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.

Covert Human Intelligence Sources

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 "CHIS"

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

Definition of a CHIS

A person is a CHIS if he/she:

establishes or maintains a personal or other relationship for the purpose of:

- obtaining information; or
- providing access to information to another person; or
- discloses information obtained by the use or existence of that relationship

RIPA authorisation is required for CHIS activity

If a CHIS is 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 a CHIS, the Authorising Officer is, by law, the Chief Executive (or in his absence either of the Assistant Chief Executives who has been nominated to act in his place).

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

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 a CHIS shall be:

- Applied for in writing ~~(or verbally in cases of urgency)~~
- 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~~.~~

The Standard Forms

Directed Surveillance

Application for directed surveillance authori~~z~~ation
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 a CHIS

Application for conduct-use of a CHIS authorisation
Application to Magistrates' Court
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 Senior Responsible Officer.

The Senior Responsible Officer's Role

The Council's Senior Responsible Officer is ***(listed in the annex to this document).***

Responsible for:

- the integrity of the process in place within the Council for the management of C~~overt~~ H~~uman~~ I~~ntelligence~~ S~~ource~~s 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 the IPCO
- ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports by the IPCO.
- Preparing and presenting reports for ~~e~~E~~lected~~ ~~m~~M~~embers~~ and presenting the policy on a regular basis to the ~~e~~E~~lected~~ ~~m~~M~~embers~~ for review.

Management of Records

The Senior Responsible Officer is responsible for ensuring a central register of authorisations 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 making regular reports to Elected Members.

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

The Senior Responsible Person is also responsible for communicating to the IPCO any unauthorised activity that might come to the attention of the authority. This must be done within 5 working days. The records, documentation, and associated documentation relating to this unauthorised activity must be retained by the Senior Responsible Officer and disclosed to the IPCO upon request, and certainly to aninspector 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.

The Elected Members are responsible for checking the consistency of the report with this policy. They will not, however, be involved in making decisions on specific authorisations.

The RIPA Monitoring Officer's Role

The Council's RIPA Monitoring Officer is **(listed in annex to this document)**.

Responsible for:

- maintaining the central register of authorisations and collating the original applications/authorisations, reviews, renewals and cancellations
- oversight of submitted RIPA documentation
- organising a RIPA training programme
- raising RIPA awareness within the Council

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 use of a 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 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 a CHIS is proportionate

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 if it 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 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 if the health and safety risks to 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 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 Department since there are other considerations in relation to management of Criminal Procedure and Investigations Act 1996 (CPIA) ~~CPIA~~ Disclosure, and use of the product of the surveillance as evidence.

Making an Application

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

The relevant forms are:

- An application for directed surveillance authori~~s~~z~~z~~ation, and/or
- An application for use of a CHIS
- An application to a Justice of the Peace

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

~~In urgent cases, verbal authorisation may be sought and authorisation recorded in writing. The same considerations and actions as set out above should be considered and recorded, and the original documents and notes provided with a reference number and submitted to the central register of records.~~

~~Cases should only be regarded as urgent if there is a likelihood of endangering life or jeopardising the investigation or operation if authorisation is not immediate. An urgent verbal authorisation may last for 72 hours. However, if the surveillance continues and there is opportunity before the expiration of 72 hours, authorisation in writing should be applied for and authorised if appropriate.~~

A Justice of the Peace may consider granting an authorisation granting an authorisation out of hours. You will need to contact the Legal Department if this is viewed as necessary.

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 an adult CHIS will last for 12 months from the date of authorisation unless renewed. It must be cancelled as soon as it is no longer required.

~~Urgent authorisation for either Directed Surveillance or use of a CHIS will last 72 hours beginning with the time when the authorisation was granted, unless subsequently endorsed by written authorisation.~~

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

During the course of an investigation the type and seriousness of offences may change. The option of authori~~s~~sing directed surveillance is dependent on the offence under investigation attracting a sentence of a 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 HumanIntelligence Sources) Order 2010 as amended, concerning the underage sale of alcohol or tobacco, an application can 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 authori~~s~~sation is already in force it should be cancelled.

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 a 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 Police and ~~A~~Criminal Evidence Act 1984 and CPIA are likely to apply to the product of the surveillance).

Updated ~~Nov 2019~~Jan 2024

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 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 CHIS to ensure that authorisation is sufficient. It is difficult to predict what might occur each time a meeting with a 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

Once the authorisation expires, surveillance must cease unless a renewal has been applied for and approved (by both the Authorising Officer and a JP).

If it appears that the directed surveillance or use of a CHIS 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 a CHIS 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.~~

Cancellations

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

Authorising Officer Responsibilities under RIPA

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

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 Officers is, by law, the Chief Executive (or in his absence one of the Assistant Chief Executives~~Corporate Directors~~).

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~~, and the OSC Procedures and Guidance~~ 2016 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.

Commented [ML3]: This document was withdrawn as was produced by organisation that no longer exists.

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 authori~~s~~zation 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 ~~and OSC Procedures and Guidance~~ 2016 both provide guidance in relation to this consideration.

Commented [ML4]: This document was withdrawn as was produced by organisation that no longer exists.

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 for preventing disorder.**

Proportionality

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. The Codes of Practice ~~and OSC Procedures and Guidance~~ 2016 both provide guidance in relation to this consideration.

Commented [ML5]: This document was withdrawn as was produced by organisation that no longer exists.

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 a CHIS

When authorising the conduct or use of 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 ("I have completed the form what do I do with it?").

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 Justice of the Peace (a District Judge or lay magistrate). If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate theyhe/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 a 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.

~~Urgent Verbal Authorisation~~

~~Urgent authorisations should not be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authority can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.~~

~~It will not be deemed urgent where the need for authorisation has been neglected or is of the officers own making.~~

~~The same matters as set out above for a written application must be considered before a verbal authorisation is granted and before it may be implemented.~~

~~It is good practice for both applicant and you to make notes of what the applicant says, and what you authorise.~~

~~Urgent authorisations last for no more than 72 hours. The original notes must be placed with the central record of authorisations. If there is a subsequent writtenauthorisation, the notes should be appended to this authorisation, and the relevant boxes within the form relating to urgent authorisation should be completed.~~

~~Upon authorisation or refusal the applicant must be made aware of exactly whatconduct has been authorised, and in the event of a refusal, or reduction in activity authorised, the reasons should be recorded on the form and communicated to the applicant.~~

~~There will still be a need to obtain a JP order before the authorisation can be implemented.~~

Authorisation Duration

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

An authorisation of use of a CHIS will last for 12 months from the date of authorisation unless renewed.

~~Urgent authorisation for either Directed Surveillance or use of a CHIS will last 72 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 forthe 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 a CHIS have not increased beyond an acceptable level.

The outcome of a consideration for 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 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 Justice of the Peace for confirmation.

The maximum time that renewal of authorisation can be approved for, is three months at a time for ~~d~~Directed ~~s~~Surveillance and 12 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 ~~d~~Directed ~~s~~Surveillance or use of a 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 ~~d~~Directed ~~s~~Surveillance or use of a 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.

Working with or through other Agencies

When some other agency has been instructed on behalf of the Council to undertake some action under RIPA, this Policy and the forms referred to 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.

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 ~~d~~Directed ~~s~~Surveillance investigation or use of a 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 a 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.

Record Keeping

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 Senior Responsible Officer.

In all cases, the following documentation must be retained:

- the application and authorisation together with (i) any supplementary documentation and notification of the approval given by the Authorising Officer and (ii) the Justice of the Peace 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 (i) the supporting documentation submitted when the renewal was requested and (ii) the requisite Justice of the Peace Order
- the date and time when any instruction was given by the Authorising Officer
- a record of the use made of any CHIS.

The Council will retain records in accordance with the Data Protection Policy.

However, records should be retained at least until the next IPCO inspection, and consideration should be given to use as evidence or unused material in pending trials or appeals.

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 CPIA~~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 not 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.

Social Networking Sites and Internet Sites

Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site, and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied, the data may be considered open source and an authorisation is not usually required.

If it necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer (i.e. the activity is more than mere reading of the site's content). ~~–~~This could occur if an officer covertly asks to become a 'friend' of someone on a social networking site.

Complaints

The R~~egulation of I~~nvestigatory P~~owers A~~~~ct~~ 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
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 OFFICERS

The following Officers, regardless of their current job titles, shall be designated Authorising Officers on behalf of the Council under the Regulation of Investigatory Powers Act 2000.

Andrew Pritchard~~Paul Turrell~~ Chief Executive

Mario Leo Corporate Head of Law and Governance

Amanda Fahey ~~Peter McKenzie~~ Assistant Chief Executive (151)

Phil Turner Assistant Chief Executive (Place)

SENIOR RESPONSIBLE OFFICER

Mario Leo ~~-~~ Corporate Head of Law and Governance

RIPA MONITORING OFFICER

Mario Leo - Corporate Head of Law and Governance

For further information, please see links below

Covert Surveillance and Property Interference revised Code of ~~Practise~~Practice

Covert Human Intelligence Sources revised Code of ~~Practise~~Practice

Code of ~~Practise~~Practice for the Investigation of Protected Electronic Information

Updated ~~Nov 2019~~Jan 2024