Surveillance & RIPA Policy

HILLINGDON
LONDON

www.hillingdon.gov.uk

Contents

1. Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) provides a statutory framework for public authorities to use surveillance and communications data, where it is necessary and proportionate for the purpose of preventing or detecting crime. RIPA regulates the use of these powers in a manner that is compatible with the Human Rights Act 1998 (HRA).

In addition to the above legislation, the Home Office has also produced Codes of Practice which provide guidance on the use of investigatory powers. The links to the codes are provided below:

Covert Human Intelligence Sources

Directed Surveillance

Communications Data

Failure to comply with this policy may make surveillance evidence inadmissible in court. An intrusion in the private or family life of an individual may also be unlawful under the Human Rights Act and may result in an investigation by the Ombudsman and/or the Investigatory Powers Tribunal.

2. Scope

This policy applies to all employees including agency, consultants and permanent staff that may wish to conduct RIPA or Non-RIPA surveillance, the use of a Convert Human Intelligence Source (CHIS) or access communication data as part of their duties of employment within the Council.

3. Principles

This policy is based on the following principles:

- To provide a framework based on legislation and codes of practice.
- To give guidance to staff on how to apply for surveillance or communications data.
- To provide knowledge and understanding on the legislative requirements investigators must follow.
- To demonstrate the Council's compliance with relevant legislation and guidance.

4. Surveillance

Background Information

In 1998 the UK introduced the Human Rights Act into legislation based on the rights set out in the European Convention of Human Rights. Under Article 8 individuals have a right to a private and family life which is regarded as a qualified right. A qualified right can be interfered with under certain circumstances. By its very nature, covert surveillance will comprise a person's article 8 rights.

RIPA therefore provides a framework to conduct covert surveillance lawfully and that is compatible with article 8. Failure to comply with RIPA whilst carrying out covert surveillance could lead to the evidence being ruled inadmissible in court, cause reputational damage to the Council and see complaints/claims being made.

RIPA provides Local Authorities with the power to carry out covert surveillance under section 28 of the act if the requirements fall within the following:

- that the authorisation is for a purpose of preventing or detecting conduct which
    - constitutes one or more criminal offences, or
    - is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one of more criminal offences; and
- that the criminal offence is/would be:
    - an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or
    - an offence under:
        a) section 146 of the Licensing Act 2003 (sale of alcohol to children); or
        b) section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children); or
        c) section 147A of the Licensing Act 2003 (persistently selling alcohol to children); or
        d) section 7 of the Children and Young Persons Act 1933 (sale of tobacco etc., to persons under 18)

Surveillance is only classed as covert if it is carried out in a way that is calculated to ensure that persons who are subject to the surveillance are unaware that it is taking place. For RIPA purposes, surveillance includes monitoring, observing or listening to persons, their movements, conversations or other activities. It may be conducted with or without assistance of a surveillance device and includes the recording of information obtained.

In law there are two types of surveillance, directed or intrusive. **Local Authorities are NOT PERMITTED to carry out intrusive surveillance.** Local Authorities can where necessary and lawful undertake directed surveillance if due process is followed.

Roles & Responsibilities

Below lists the details of those that are responsible for any applications relating to RIPA:

- Senior Responsible Officer (SRO) – Glen Egan Head of Legal Services
- Authorising Officers (AO) – Alex Brown Head of Counter Fraud, Stephanie Waterford Head of Public Protection & Enforcement
- Central record & Co-ordinating Officer – Glen Egan Head of Legal Services *(Role to be delegated in Legal Services at a later date)*

Directed & Intrusive Surveillance

Directed and Intrusive surveillance are defined in RIPA under section 26 of the act as the following:

- for the purposes of a specific investigation or operation;
- in such a manner as is likely to result in the obtaining of private information about a person (whether one specifically identified for the purposes of the investigation or operation); and
- otherwise, than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of surveillance.

Intrusive Surveillance is defined by section 26(3) of RIPA as covert surveillance that:

- is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Private Information

During any activity under RIPA there is a possibility you will collect private information. Under RIPA private information relates to any data obtained regarding a person's private or family life. Private information may also include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate. However, consideration should always be given to whether there are any other lawful and less intrusive means of obtaining personal data.

Consideration should be given to the collection of private information when seeking authorisation. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or where one or more pieces of information (whether or not in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person. In such circumstances, the totality of information gleaned may constitute private information even if the individual records do not. Where such conduct includes covert surveillance, an authorisation for directed surveillance should be sought.

Remember, this Procedure Manual deals with RIPA and Non-RIPA authorisations so even if you do not meet the criminal threshold and would not be able to apply to the Magistrates Court for authorisation, you will still be required to complete the relevant documents as a Non-RIPA request and this paperwork and thought process should still be captured on the relevant forms and recorded on the central RIPA register.

When authorisation is not required

In some cases, surveillance activity may not constitute directed surveillance and therefore not require authorisation. This includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- overt use of CCTV and ANPR systems

During an investigation events may unfold which requires an immediate response by officers to conduct directed surveillance. RIPA is not intended to prevent law enforcement officers fulfilling their legislative functions. However, forms for authorisation should be completed at the earliest opportunity after the event. If you need assistance or advice, please contact Legal Services.

5. Covert Human Intelligence Source (CHIS)

Background Information

A person is a Covert Human Intelligence Source (or CHIS) if:

- he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating anything falling within the circumstances below:
- he covertly uses the relationship to obtain information or to provide access to any information to another person; or
- he covertly discloses information obtained using or because of such a relationship.

In some circumstances an individual who provides information voluntarily may become a CHIS as per Section 26(8)c of RIPA. Officers should be mindful of this when receiving information, however this unlikely if the individual only gives information on a one-time basis.

It is important for officers to understand the difference between “establish” and “maintain” as mentioned above. “Maintain” requires endurance over a period of time where as “establish” is the setting up of a relationship.

Authorisation is needed for use or conduct of a CHIS. Though they seem to be the same, there are slightly differences between use and conduct. The “conduct” of a CHIS is an authorisation for conduct which will authorise steps taken by a CHIS, on behalf of, or at the request of, the Council. The “use” of a CHIS involves any action on

behalf of the Council to induce, ask or assist a person to engage in the said conduct of a CHIS, or to obtain information by means of that conduct.

General Rules on Application & Authorisation of a CHIS

The use or conduct of a CHIS requires authorisation as it is classed a covert surveillance, the application and process is broadly in line with applying for directed surveillance, including the fact that an authorisation may only be granted where such surveillance is necessary on one of the statutory grounds; that any such use of a CHIS must be reasonable and proportionate, and that due consideration should be given to collateral intrusion. Judicial approval is also required.

A written authorisation last for 12 months, however this can be extended where reasonable proportionate and necessary to do so. The application, review, cancellation, or extension process of a CHIS is explained in further details in Section 6.

When applying for or granting authorisation officers must consider local and community impacts. During the application process officers must note any sensitivities within the community that may have a bearing or impact of the use or conduct of a CHIS. This includes other similar activities already been undertaken including existing deployment of other CHIS. If a conflict arises the Authorising Officer should discuss with the Senior Responsible Officer and any other relevant public body.

There is a requirement for elected members of the Council to review the use of RIPA every 12 months and to set the policy and this includes a review of the Council's use of any CHIS.

Management of a CHIS

Not only must you satisfy that the authorisation of a CHIS is necessary for the purpose of preventing and detecting crime, but you must also ensure the use or conduct is proportionate in what you are trying to achieve. An AO should not grant an authorisation unless they believe arrangements are in place for the following:

- that there will always be a person who will have day-to-day responsibility for dealing with the source on behalf of the Council and for the source's security and welfare. This person is known as the Handler and is responsible for dealing with the CHIS on behalf of the authority; directing the day-to-day activities of the CHIS; recording the information supplied and monitoring the CHIS's security and welfare. The Handler would usually hold a rank or position lower than the AO;
- that there will always be another person who will have general oversight of the use made of the source. This person is known as the Controller and will be responsible for the management and supervision of the Handler and general oversight of the use of the CHIS. Obviously, this must be someone other than the Handler and ideally should be someone other than the AO, but due to the relatively small size of the Council's enforcement teams, the AO is likely to be the Controller.

- that the Handler will have responsibility for maintaining a record of the use made of the source.
- that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters as are specified in regulations made by the Secretary of State, (see below); and
- that records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

Particulars to include in records

The Secretary of State has made the Regulation of Investigatory Powers (Source Records) Regulations 2000. The following particulars must be included in the records relating to each source:

- the identity of the source and any other identities, if known
- any relevant investigating authority (if different from the authority maintaining the records;
- the means by which the source is referred to in each authority;
- any other information connected with the security and welfare of the source;
- any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information above has been considered and that any identified risks to the security and welfare of the source have been properly explained to and understood by the source;
- the date and circumstances in which, the source was recruited;
- the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a)-(c) of RIPA or in any order made under section 29(2)(c);
- the periods during which those persons have discharged those responsibilities;
- the tasks given to the source and the demands made of him in relation to his activities as a source;
- all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- the information obtained by each relevant investigating authority by the conduct or use of the source;
- any dissemination by that authority of information obtained in that way;
- in the case of a source who is not an undercover operative, [an enforcement officer within the Council] 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.

6. Authorisation Procedures: Directed Surveillance & CHIS

Background & Overview

In ordered to carry out directed surveillance or the deployment of a CHIS, officers must follow the procedures set out in this section to gain lawful authorisation. All forms

relating to authorisation can be found in Appendix A. A brief overview of this section is provided below:

- Obtain relevant application form from this policy or via Intranet page or by contacting the Fraud email address.
- Complete application form ensuring statutory grounds and legal thresholds are met.
- Send application form to an AO to review. The AO should be from a different department. AOs should not review applications from own departments or investigations they are involved in.
- Applications to be lodged on central register and all documentation leading to decision.
- RIPA Co-ordinating Officer to allocate a URN to be used throughout the case
- If the relevant AO approves the application and it triggers a need to go to the Magistrates, then Legal will contact the local Magistrates' Court to arrange a hearing date
- The authorisation and surveillance should not begin until the court has granted the application. An initial authorisation is valid for a period of three months and should be reviewed throughout the three months and either cancelled or renewed using the appropriate forms set out below.

Application Form

A written application for authorisation for Directed Surveillance and CHIS should describe the conduct to be authorised and the purpose of the investigation or operation. It should also include:

- the reason why the surveillance is necessary;
- the reasons why it is proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained because of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance;
- a subsequent record of whether the authorisation was given or refused, by whom and the date and time.

An example of the application for authorisation of directed surveillance or CHIS forms are attached to this policy (see **Appendix A**).

AOs must not authorise investigations in which they are directly involved. It is recommended that AOs do not authorise applications that come from their own department and that another AO from a different department considers the application.

Legal thresholds: Necessity and Proportionality

Obtaining an authorisation in accordance with RIPA will only be a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for directed surveillance to be undertaken. The AO may only authorise surveillance which is necessary on statutory grounds and s/he must also be satisfied that covert surveillance is necessary in the circumstances of the case. Once the AO has determined that the proposed activities are necessary, s/he must be satisfied that they are proportionate to the overall aim of the investigation.

Proportionality is a key concept of RIPA. An authorisation should demonstrate how an AO has reached the conclusion that the activity is proportionate to what it seeks to achieve, including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate. Failure to adequately address this issue could see the authorisation falling foul of the RIPA quality procedures, potentially resulting in the surveillance being challenged or suspended.

The activity will not be proportionate if it is excessive in the circumstances of the case or if the information that is being sought could be obtained by other less intrusive means. As an example of proportionality, a person can claim self-defence to a charge of assault where he has used reasonable force to protect himself; it may be proportionate to kick and punch an assailant armed with a knife, but it would not be proportionate to use a knife or a gun against an unarmed attacker.

In determining whether surveillance is proportionate, the AO should make clear that the four elements of proportionality have been fully considered:

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
- 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 method for obtaining the necessary result, and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented

Authorisation Form

The completed Application form should be given to the AO. The Authorisation form is a separate form and is the only document which should be reviewed by a court during a trial where a dispute arises as to whether evidence obtained by way of covert surveillance was obtained lawfully. This document must include all relevant information to ensure it can be presented as a standalone document to justify why the surveillance has been undertaken.

The AO should, therefore, record on the Authorisation form the full extent of what is authorised i.e. who, what, why, when, where and how, including an independent authorisation for any technical equipment which is to be used and the location of such equipment. This will ensure that the specific parameters of what has been duly

authorised is then passed to the Applicant/ officer carrying out the surveillance. The AO should also explain why he is satisfied that the directed surveillance is necessary and proportionate in the circumstances of the case before he endorses the Authorisation. Caution should be taken not to copy/paste or use old or earlier versions of the same form for other authorisations.

If the authorisation is refused, the AO should clearly mark on the form the reasons for refusal and any comments that may assist the Applicant Officer to reconsider the proposals and resubmit a fresh application. Copies of such refusals must also be sent electronically to the RIPA Co-ordinating Officer. Again, caution should be taken not to copy/paste or use old or earlier versions of the same form. The authorisation form can be found in **Appendix A** of this policy.

A written authorisation for Directed Surveillance is initially valid for three months from the day on which it took effect, i.e. from the date of Judicial Approval, but can be renewed within that time, though any renewal will require judicial approval.

Reviews

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. In each case the relevant AO should determine how often a review should take place during the lifetime of any authorisation and should then undertake the review him/herself.

Any proposed or unforeseen changes to the nature or extent of the surveillance operation should also be brought to the attention of the AO by means of a review. The AO should consider whether the proposed changes are proportionate before approving or rejecting them. The review form is attached to the Manual as **Appendix A**.

Renewals

An authorisation may be renewed for a further period of three months and can be renewed more than once, if the AO considers it necessary for the authorisation to continue and judicial approval is in place. The renewal form is attached to this manual as Appendix A. It can also be obtained from the intranet page.

All requests for renewals should record:

- whether it is the first renewal, if not list all previous occasions when renewed;
- any significant changes to the information given in the original authorisation;
- the reasons why it is necessary to continue with the surveillance and that it is still proportionate to the aim being sought;
- the content and value to the investigation or operation of the information so far obtained by surveillance;
- the results of regular reviews of the investigation or operation

Cancellations

If, during the currency of an authorisation, the AO is satisfied that the authorisation is no longer necessary, s/he must cancel it. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. Judicial Approval is not required to cancel an authorisation.

The AO must inform those carrying out the surveillance and the date and time of this notification should be recorded on the Cancellation Form. The cancellation form is attached to this Manual as **Appendix A**.

A Cancellation Form must be completed in all cases. Cancellations should also include the reason for cancellation as well as the result of the operation, and they must also be noted on the central record of authorisations.

Obtaining Judicial Approval

From 1st November 2012 judicial approval of all local authority authorisations and renewals (for both directed covert surveillance and the use of a CHIS), is required from the Magistrates' Court. Authorisations and renewals are invalid and cannot be acted upon until the approval of the Court has been given.

The Magistrates' Court may give approval only if it is satisfied that:

- authorisation is necessary for the prevention or detection of crime; and
- that authorised surveillance would be proportionate to what is sought to be achieved by carrying it out; and;
- the AO was an individual designated for the purpose, i.e. Director, Head of Service, Service Manager, or equivalent; and
- the crime being investigated carries a minimum prison sentence of 6 months, or concerns the sale of alcohol to children, or allowing the sale of alcohol to children, or persistently selling alcohol to children, or selling tobacco to children; and
- at the time of the application to the Magistrates' Court there remains reasonable grounds for believing that the above conditions are met

The Council is not required to give notice of the intended application to the person(s) who are the subject matter of the surveillance nor their representatives.

Making the Application

After an application has been authorised by the AO, Legal Services/Applicant Officer will contact the Local Magistrates' Court to arrange a hearing. The AO should provide the Court with a copy of the original application, the authorisation and any supporting documents setting out the case. In addition, the investigating officer should provide the Court with a partially completed judicial application (see **Appendix A**). This forms the basis of the application to the Court and should contain all information that is relied upon. The original RIPA authorisation or notice should be shown to the court but should be retained by the Council so that it is available for inspection by the

Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The hearing will be in private and heard by a single Justice of the Peace who will read and consider the RIPA authorisation and the judicial application form.

The Justice of the Peace will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation 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 AO 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. If more information is required to determine whether the authorisation or notice has met the tests, the court will refuse the authorisation.

Following consideration of the case the court will provide their decision. This can be one of the following:

- Approve the Grant or renewal of an authorisation
- Refuse to approve the grant or renewal of an authorisation
- Refuse to approve the grant or renewal and quash the authorisation

7. Communications Data

The Investigatory Powers Act 2016 (IPA) came into force from 30 December 2016 and replaces Part I of Chapter II of RIPA for Communications Data. There is a separate code of practice on the use of communications data, with additional guidance issued on the use of communications data in April 2023.

IPA governs the accessing of communications data from Communication Service Providers (CSP). It does NOT allow for interception of communications (e.g. bugging of telephones etc.). **Local authorities are not permitted to intercept the content of any person's communications**. It is an offence to do so without lawful authority.

The term communications data embraces the 'who,' 'when' and 'where' of a communication but not what was written or said (i.e. not the content). It includes the manner in which and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on with the communication.

Communications data is generated, held, or obtained in the provision, delivery, and maintenance of postal or telecommunications services.

There are two categories of communications data. These are Events Data and Entity Data. The Council only has power to acquire Entity Data or Events Data. A local authority cannot acquire internet connection records such as details of the internet service, website, or instant messaging service, that a specific device has connected to.

EVENTS DATA	ENTITY DATA
• Periods of subscription/use • Telephone call records • Information about the provision of conference calling, call messaging, call waiting and call barring services • Timing and duration of service usage (calls and /or connections) • Connection/Disconnection information • Records of connections to internet services • Information about amounts of data downloaded and/or uploaded • Provision and use of forwarding/redirection services • Records of postal items e.g. registered, recorded or special delivery postal items • Top-up details for mobile phones - credit/debit card details and voucher/e-top up details	• Name of account holder/ subscriber • Billing, delivery and installation address(es) • Contact telephone number(s) • Bill payment arrangements including bank/credit card details • Collection/delivery arrangements from a PO box • Services subscribed to by the customer • Other customer information such as any account notes, demographic information or sign-up data (not passwords)

Serious Crime

Where the purpose of the acquisition is to prevent or detect crime, and the data required is Events Data, the offence must meet at least one of the definitions of serious crime:

- An offence that carries a prison sentence of 12 months or more
- An offence by a corporate body
- An offence falling within the definition of serious crime in section 81(3)(b) of IPA 2016 (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose)
- An offence in which the sending of a communication is an integral part
- An offence in which a breach of a person's privacy is an integral part

Procedure for obtaining communications data

The procedure to obtain communications data has been overhauled by IPA and is now processed by two organisations. These are:

<u>The National Anti-Fraud Network (NAFN)</u>

NAFN is hosted by Tameside Metropolitan Borough Council and acts as a Single Point of Contact (SPoC) for local authorities. NAFN provides a SPoC service to the Council allowing NAFN to act as a source of expertise, with designated officers responsible for reviewing applications. All applications for Communication data must be submitted to

NAFN who will assist and advice the Council and submit the applications to OCDA once they are satisfied with the contents of the application/surveillance.

Office for Communications Data (OCDA)

OCDA became part of the Investigatory Powers Commissioner's Office (IPCO) in March 2024. IPCO provides independent oversight of the use of investigatory powers.

The procedure to obtain communications data at Hillingdon Council are as follows:

- Prepare a draft application. Once done, an Approved Rank Officer (ARO) should review and be made aware of the application. The details of the AROs are at paragraph two above.
- Login into the NAFN portal. Each department should have their own login details.
- Ensure that the application form is completed thoroughly, and the statutory grounds of proportionality, reasonableness and lawfulness are met.
- Once the ARO is satisfied, Applicant Officer to send the application via the NAFN portal.
- The accredited advisers at NAFN will scrutinise the application independently and provide advice to the Applicant ensuring it acts in an informed and lawful manner. Once NAFN is satisfied with the application, they will submit the application to OCDA.
- If the application has been granted, NAFN will be notified and serve a notice on the relevant CSP requiring them to provide the information on behalf of the Council.

8. Non-RIPA Surveillance

Following the introduction of the "serious crime threshold" the legal protection offered by RIPA to local authorities is no longer available in cases where the criminal offence under investigation is not punishable by at least 6 months imprisonment or relates to the sale of underage products such as alcohol, tobacco or nicotine inhaling products. However, this does not mean that it will not be possible to investigate lesser offences or other non-criminal matters with a view to protecting the victim or stopping the offending behaviour, or that surveillance cannot be used in such investigations. The statutory RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble 'hotspots,' immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

Whilst authorisation under RIPA affords a public authority a defence under Section 27 (i.e. the activity is lawful for all purposes), failure to obtain an authorisation does not make covert surveillance unlawful, however. Section 80 RIPA states:

"Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation, or notice, or by virtue of which information may be obtained in any manner, shall be construed—

(a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;
(b) as otherwise requiring:
(i) the issue, grant or giving of such a warrant, authorisation or notice, or
(ii) the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice, before any such conduct of that description is engaged in; or
(c)as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act."

This point was explained more fully by the Investigatory Powers Tribunal in the case of C v The Police (Case No: IPT/03/32/H 14th November 2006):

"Although RIPA provides a framework for obtaining internal authorisations of directed surveillance (and other forms of surveillance), there is no general prohibition in RIPA against conducting directed surveillance without RIPA authorisation. RIPA does not require prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful."

Non-RIPA Surveillance Authorisation Procedure

The rules and regulations in relation to RIPA authorisations apply to non-RIPA applications, without, of course, the requirement to seek judicial approval. This is to ensure that officers are not using covert surveillance arbitrarily and excessively for the reasons set out above. Officers must therefore ensure that, when they are considering conducting covert surveillance that does not fall within the remit of RIPA, that they do so in the same way as they would when seeking a RIPA authorisation. Please see **Appendix A** for a template of the 'Non-RIPA Surveillance Form.'

The Non-RIPA Authorisation form at the end of this appendix, together with the renewal and cancellation forms for RIPA surveillance can be used for both RIPA and Non-RIPA surveillance. The surveillance should cease as soon as the surveillance is no longer necessary, and a Cancellation form should be completed.

As with Directed Surveillance and CHIS, Non-RIPA authorisation and cancellation forms should be provided to the RIPA Coordinator who will maintain a central record of such authorisations/cancellations.

9. Use of social media

Officers checking Facebook, Instagram, Twitter and other forms of social media as part of an investigation, need to be aware that such activity may be subject to RIPA either as directed surveillance or deploying a CHIS. Browsing public open web pages where access is not restricted to "friends", followers or subscribers is not covert activity provided the investigator is not taking steps to hide her/his activity from the suspect. The fact that the suspect is or may be unaware of the surveillance does not make it covert. However, any surveillance activity carried out in a manner which is calculated to ensure that a person subject to surveillance is unaware that surveillance against

them is taking place is activity which is covert, and you will need to consider obtaining a RIPA or NON-RIPA authorisation.

Officers must not covertly access information on social media, which is not open to the public, for example by becoming a “friend’ of a person on Facebook or communicating via social media with the suspect as this type of activity conducted in a covert manner would engage the CHIS provisions. An example of non-permitted covert surveillance is the creation of a fake profile.

The growth of the internet, and the extent of the information that is now available online, presents new opportunities for local authorities to view or gather information which may assist officers in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual’s online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered. Where a person acting on behalf of the authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person’s private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

The gathering and use of online personal information by the Council will engage Human Rights particularly the right to privacy under Article 8 ECHR. To ensure such rights are respected the Data Protection Act must also be complied with. Please consult with the Council's Data Protection Officer or Legal Services if you wish to discuss the use of social media as part of an investigation.

10. General Information

Central Record Keeping

A record of the following information pertaining to all authorisations shall be centrally retrievable for a period of at least three years from the ending of each authorisation, though it is desirable and recommended to keep records for five years. This information should be regularly updated whenever an authorisation is granted, reviewed or cancelled and should be made available to the relevant Commissioner or an Inspector from IPCO upon request. The central Record should be a mirror image of each decision made, and documentation gathered, during the entire case.

The following information should be included:

- the type of authorisation
- the date the authorisation was given
- name and rank/grade of the AO
- the unique reference number (URN) of the investigation or operation
- the title of the investigation or operation, including a brief description of the names of subjects, if known
- details of attendances at the magistrates' court if the application is for RIPA surveillance
- the dates of any reviews
- if the authorisation had been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the AO
- whether the investigation or operation is likely to result in obtaining confidential information as defined in the Home Office Code of Practice
- whether the authorisation was granted by an individual directly involved in the investigation
- the date the authorisation was cancelled

All authorisations granted by individual AOs, on behalf of the Council, must be sent electronically to the RIPA Co-ordinating Officer. The RIPA Co-ordinating officer will be responsible for updating this record whenever an authorisation is granted, renewed, reviewed or cancelled. This record must be made available to the relevant Commissioner or an Inspector upon request.

Retention and Destruction

Where surveillance footage could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. Particular attention is also drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

RIPA does not prevent material obtained from properly authorised surveillance being used in other investigations. Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance.

AOs must ensure compliance with the appropriate data protection requirements and any relevant codes relating to the handling and storage of material.

Training

Both AOs and those applying for authorisations should attend regular training sessions to ensure they are being kept up to date with any developments, both procedurally and legally. As a matter of good practice, the training should take place every year with regular meetings of AOs held throughout the year.

Complaints

The Investigatory Powers Tribunal was set up to investigate and decide upon complaints made to them within its jurisdiction, including complaints made by a person who is aggrieved by any conduct to which Part II of RIPA applies, where he believes such conduct to have taken place in "challengeable circumstances" or to have been carried out by or on behalf of any of the intelligence services.

Conduct takes place in "challengeable circumstances" if it takes place:

- with the authority or purported authority of an authorisation under Part II RIPA; or

- the circumstances are such that it would not have been appropriate for the conduct to take place without authority; or at least without proper consideration having been given to whether such authority should be sought.

Further information on the exercise of the Tribunal's functions and details of the relevant complaints procedure can be obtained from:

Investigatory Powers Tribunal
PO Box 33220
London SW1H 9ZQ.
Tel: 0207 035 3711
E: info@ipt-uk.com

In addition, members of the public will still be able to avail themselves of the Council's internal complaints procedure, where appropriate, which ultimately comes to the attention of the Local Government Ombudsman.

Inspection & Oversight

The Act also provides for the independent oversight and review of the use of the powers contained within Part II of RIPA, by a duly appointed Chief Surveillance Commissioner. The Investigatory Powers Commissioner's Office (IPCO) is now responsible for the judicial oversight of the use of covert surveillance by public authorities throughout the United Kingdom.

There is a duty on every person who uses the powers provided by Part II of RIPA, which governs the use of covert surveillance or covert human intelligence sources, to disclose or provide to the Chief Commissioner (or his duly appointed Inspectors) all such documents and information that he may require for the purposes of enabling him to carry out his functions.

11. Administration

Policy number	**CFT002**	**Version number**	**1.0**
Effective date	**26th April 2024**	**Date of last revision**	**1st April 2024**
Policy owned by	**Alex Brown**	**Policy approved by**	**Cabinet**

Version History

Version	Approved by	Revision date	Description of change	Author
1.0	**Cabinet**	**1st April 2024**	**Review & format update**	**Alex Brown**

12. Appendix A – RIPA Forms

Unique Reference Number (URN)	

APPLICATION FOR DIRECTED SURVEILLANCE AUTHORITY
(TO BE COMPLETED BY THE OFFICER MAKING THE APPLICATION/EAD OFFICER IN THE CASE)
Part II Regulation of Investigatory Powers Act 2000

Position	
Department	
Address	
Telephone Number	
Name of Applicant	
Email address	
Operation Name (if applicable)	
Date	

1. Authority Required From:
Head of Service/ YES/NO Service Manager or equivalent (delete as appropriate)
Head of Paid Service/ Chief Officer (Confidential Material Only) YES/NO

2. Background Information
a) Describe the purpose of the specific investigation/ operation.
b) Describe in detail the surveillance operation to be authorised, including any premises or vehicles which will be included in the surveillance or technical equipment (camera, binoculars, sound recorder, fixed cameras) that may be used for the surveillance. Give the expected duration of the surveillance and location of any such equipment. Where appropriate, a map can be attached to this application to denote the area within which the surveillance is to take place.

c) Outline the information expected to be obtained from this activity.
3. Particulars/ details (where known) of subject (s) against whom this surveillance is directed.

• Name • Alias • DOB • Address • Any other relevant information	• Name • Alias • DOB • Address • Any other relevant information

4. Necessity
Directed Covert Surveillance can only be undertaken by the Council where the surveillance is **necessary for the purpose of preventing or detecting crime or preventing disorder** (Section 28(3)(b)). Explain <u>why</u> this surveillance is necessary on this ground giving specific details of the alleged crime and/or disorder.

5. Proportionality
Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? Why is this intrusion outweighed by the need for surveillance in operational terms? Can the evidence be obtained by any other less intrusive means? If not, why not?
6. Collateral Intrusion
Supply details of any potential collateral intrusion and why that intrusion is unavoidable.
What steps do you intend to take to minimise this collateral intrusion?

7. Confidentiality
Assess the likelihood of acquiring confidential material, such as • Legal Privilege • Confidential Personal Information • Spiritual Counselling • Confidential Journalistic Material

8. Other operations
Are there any other operations/investigations being undertaken or planned by other departments/ public authorities e.g. Police which could impact on the deployment of surveillance or compromise the proposed activity?

9. Applicant			
Name		Position	
Signature		Date	

Unique Reference Number (URN)	

Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)

(TO BE COMPLETED BY THE OFFICER MAKING THE APPLICATION/ LEAD OFFICER IN THE CASE)

Part II Regulation of Investigatory Powers Act 2000

Position	
Department	
Address	
Telephone Number	
Name of Applicant	
Email address	
Operation Name (if applicable)	
Date	

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail <u>the purpose</u> for which the source will be tasked or used.
4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.
5. Identify on which grounds the conduct or the use of the source is <u>necessary</u> under Section 29(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (e.g. SI 2010 No.521*).
• In the interests of national security;

- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

6. Explain <u>why</u> this conduct or use of the source is necessary on the grounds you have identified

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable.
Describe precautions you will take to minimise collateral intrusion and how any will be managed.

8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source

9. Provide an assessment of the risk to the source in carrying out the proposed conduct

10. Explain <u>why</u> this conduct or use of the source is proportionate to what it seeks to achieve.
How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means?

11. Confidential information
Indicate the likelihood of acquiring any confidential information.

References for any other linked authorisations:

12. Applicant's Details.

Name (print)		**Grade/Rank/Position**	
Signature		**Tel No:**	
Date			

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.

14. Explain <u>why</u> you believe the conduct or use of the source is necessary and **Explain <u>why</u> you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement**
15. Confidential Information Authorisation. Supply details demonstrating compliance with the Code

16. Date of first review:	

17. Programme for subsequent reviews of this authorisation. Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.

18. Authorising Officer's Details			
Name (Print)		**Grade/Rank/Position**	
Signature		**Time and date granted*** **Time and date authorisation ends**	

Unique Reference Number (URN)	

AUTHORISATION FOR DIRECTED SURVEILLANCE AUTHORITY

(TO BE COMPLETED BY AUTHORISING OFFICER)

Part II Regulation of Investigatory Powers Act 2000

Position	
Department	
Address	
Telephone Number	
Name of Applicant	
Email address	
Operation Name (if applicable)	
Date	

3. Authority Required From:	
Head of Service/ Service Manager or equivalent (delete as appropriate)	YES/NO
Head of Paid Service/ Chief Officer (Confidential Material Only)	YES/NO

2. Necessity
Directed Covert Surveillance can only be undertaken by the Council where the surveillance is **necessary for the purpose of preventing or detecting crime or preventing disorder** (Section 28(3)(b)). Explain why this surveillance is necessary on this ground and why you are satisfied that covert surveillance is necessary in the circumstances of this particular case.
3. Proportionality
Explain why you are satisfied that the proposed activity is proportionate to the aim that it seeks to achieve. In determining whether surveillance is proportionate, you should make it clear that the following four elements of proportionality have been fully considered:
i) Demonstrate how the size and scope of the operation has been balanced against the gravity and extent of the perceived mischief:

ii) Explain how and why the methods to be adopted will cause the least possible intrusion on the target and others:

iii) Show that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result:

iv) Evidence what other methods have been considered and why they were not implemented.

4. Application Granted where confidential information <u>is not</u> likely to be acquired. Authorising Officer's Statement

This should include a detailed summary of the surveillance that is being authorised – whom the surveillance is directed against, where and when it will take place, what surveillance is to take place, why such surveillance is authorised and how it will be carried out, *including a separate authorisation for any technical equipment which is to be used in support of the directed surveillance.*

I hereby authorise the directed surveillance as specified above*

This written authorisation will cease to have effect at the end of **3 months** unless renewed (see separate form for renewals)*

This authorisation will be reviewed frequently to assess the need for the authorisation to continue*

*delete if authorisation refused.

Name		**Position**	
Signature			
Date of first review		**Date of Expiry = 3 months from grant, e.g. granted 1st Jan expires 31st March**	

5. Endorsement by the officer carrying out the surveillance

NOTE: Before signing this endorsement, the person carrying out the surveillance must be satisfied that s/he understands the parameters of the surveillance being authorised and that all relevant information relating to that surveillance is contained within Section 4 above.

I hereby endorse the authorisation to confirm my understanding of the surveillance that is being authorised.			
Name		**Position**	
Signature		**Date**	
Date of first review		**Date of Expiry = 3 months from grant, e.g. granted 1st Jan expires 31st March**	

6. Application Refused – Authorising Officer's Statement			
NOTE: If you consider that the surveillance is not necessary or proportionate to the aim it is seeking to achieve, or that more information is needed before a decision can be made, you should refuse to authorise giving your reasons in the space below			
I hereby refuse the application for directed surveillance for the reasons given above * ***delete if authorisation granted**			
Name		**Position**	
Signature		**Date**	

<u>Boxes 7, 8 and 9 should only be completed when confidential information is likely to be acquired.</u>

7. Application Granted <u>where confidential information is likely to be acquired</u> NB: to be completed by the <u>Head of Paid Service or Chief Officer</u> - see Chapter 4 of the Home Office Revised Code of Practice.
Authorising Officer's Statement: This should include a detailed summary of the surveillance that is being authorised – whom the surveillance is directed against, where and when it will take place, what surveillance is to take place, why such surveillance is authorised and how it will be carried out, *including a separate authorisation for any technical equipment which is to be used in support of the directed surveillance and* confirm the likelihood of obtaining confidential information

I hereby authorise the directed surveillance as specified above*

This written authorisation will cease to have effect at the end of **3 months** unless renewed (see separate form for renewals)*

This authorisation will be reviewed frequently to assess the need for the authorisation to continue*

*delete if authorisation refused.

Name		**Position**	
Signature		**Date**	
Date of first review		**Date of Expiry = 3 months from grant, e.g. granted 1st Jan expires 31st March**	

8. Endorsement by the officer carrying out the surveillance <u>where confidential information is likely to be acquired</u>			
NOTE: Before signing this endorsement, the person carrying out the surveillance must be satisfied that s/he understands the parameters of the surveillance being authorised and that all relevant information relating to that surveillance is contained within Section 4 above.			
I hereby endorse the authorisation to confirm my understanding of the surveillance that is being authorised.			
Name		**Position**	
Signature		**Date**	
Date of first review		**Date of Expiry = 3 months from grant, e.g. granted 1st Jan expires 31st March**	

9. Application Refused – by Head of Paid Service or Chief Officer <u>where confidential information is likely to be obtained</u>			
NOTE: If you consider that the surveillance is not necessary or proportionate to the aim it is seeking to achieve, or that more information is needed before a decision can be made, you should refuse to authorise giving your reasons in the space below			
I hereby refuse the application for directed surveillance for the reasons given above * ***delete if authorisation granted**			
Name		**Position**	
Signature		**Date**	

Unique Reference Number (URN)	

REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION

(TO BE COMPLETED BY AUTHORISING OFFICER)

Part II Regulation of Investigatory Powers Act 2000

Position	
Department	
Address	
Telephone Number	
Name of Applicant	
Email address	
Operation Name (if applicable)	
Date	

1. Authorisation/ Renewal			
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	

2. Details of review			
Is this the first review?	YES/NO		
If NO, how many times has the authorisation been reviewed		Date of last review	

3. Summary of the investigation/ operation to date and the value of the information so far obtained.

4. Necessity
Detail the reasons why it is necessary to continue with the directed surveillance.

5. Proportionality
Explain how the directed surveillance is still proportionate to what it seeks to achieve. You should consider what information has already been gathered and balance the intrusiveness of the continued activity against the need for action in operational terms, taking into account whether the activity is excessive in the circumstances of the case or if the information still to be sought could be obtained in a less intrusive way.

6. Confidentiality
Give details of any confidential information acquired or accessed and the likelihood of acquiring further confidential information

7. Collateral Intrusion
Detail any incidents of collateral intrusion and the likelihood of further collateral intrusion.

8. Applicant			
Name		Position	
Signature		Date	

9. Authorising Officer's Comments
Specify the ongoing parameters of the surveillance should you be satisfied that the surveillance should continue. You cannot broaden the scope of any application for surveillance but you may limit it if you believe this is justified in the circumstances of the case.

10. Authorising Officer's statement			
I hereby agree that the directed surveillance investigation/ operation as detailed above [should/ should not] continue [until the next review/renewal /it should be cancelled immediately].			
Name		Position	

Signature		Date	

11. Date of Next Review	

Unique Reference Number (URN)	

APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE AUTHORITY

(TO BE COMPLETED BY THE ORIGINAL APPLICANT/ LEAD OFFICER IN CASE)

Part II Regulation of Investigatory Powers Act 2000

Name of Applicant	
Position	
Department	
Address	
Telephone Number	
Email address	
Operation Name (if applicable)	
Date	

1. Renewals	
Has this authorisation been renewed before?	YES/NO
If YES, how many times?	
List the date(s) for all previous renewals	

2. Summary of the investigation/operation to date and the value of the information so far obtained.
3. Has there been any significant change to the information that was provided for the original authorisation? If YES give details.

4. Necessity
Detail the reasons why it is **necessary for the prevention or detection of crime or prevention of disorder,** as well as why it is necessary in the circumstances of this case, to continue with the directed surveillance in this operation.

5. Proportionality

Is the directed surveillance still proportionate to the aim that it seeks to achieve? You should consider what information has already been gathered and balance the intrusiveness of the continued activity against the need for action in operational terms, taking into account whether the activity is excessive in the circumstances of the case or if the information still to be sought could be obtained in a less intrusive way.

6. Confidentiality
Give details of any confidential information acquired or accessed and the likelihood of acquiring further confidential information

7. Collateral Intrusion
Detail any incidents of collateral intrusion and the likelihood of further collateral intrusion, including steps to be taken to minimise such intrusion

8. Reviews	
How many reviews have there been since the original authorisation was granted?	
Date	Results of review

9. Applicant			
Name		Position	
Signature		Date	

10. Authorising Officer's comments
Explain in your own words why the directed surveillance [is still/ is no longer] necessary and proportionate. You should be satisfied that the activity is not excessive in the circumstances of the case and that the information being sought could not be obtained in any other way.

11. Authorising Officer's statement			
I hereby [authorise/ refuse to authorise] the renewal of the directed surveillance operation as detailed above. [The renewal of this authorisation will last for 3 months/ The authorisation should be cancelled immediately]* . This authorisation will be reviewed frequently to assess the need for the authorisation to continue. *if cancelled, a Cancellation Form should be completed immediately.			
Name		Position	
Signature		Date	

12. Date of next review	

Unique Reference Number (URN)	

CANCELLATION OF DIRECTED SURVEILLANCE

(TO BE COMPLETED BY AUTHORISING OFFICER)

Part II Regulation of Investigatory Powers Act 2000

Position	
Department	
Address	
Telephone Number	
Name of Applicant	
Email address	
Operation Name (if applicable)	

1. Renewals			
Was the authorisation renewed?		YES/NO	
If YES, how many times?		Date of last renewal	

2. Details of Cancellation
Explain the reason(s) for cancelling the authorisation for directed covert surveillance

3. Intelligence update
a) Provide details of the evidence obtained through the directed surveillance since the initial authorisation was granted/ last renewal
b) What value was this evidence to the investigation?

4. Give details of outcome of investigation to include the nature of any proceedings instituted or intended to be instituted.

5. Product of Surveillance
a) Arrangements for the storage of material obtained by the surveillance

b) Arrangements for its review and destruction when no longer of use
c) Arrangements for the immediate destruction of unrelated material obtained by way of collateral intrusion.
d) Give details of any confidential material acquired and how it has been stored

6. Applicant			
Name		Position	
Signature		Date	

7. Authorising Officer's cancellation			
I hereby cancel the authorisation for directed surveillance with immediate effect.			
Name		Position	
Signature		Date	

Unique Reference Number (URN)	

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

Local authority: .....

Local authority department .....

Offence under investigation .....

Address of premises or identity of subject: .....

Covert technique requested: (tick one and specify details)

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

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

Investigating Officer: .....

Authorising Officer: .....

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

Address of applicant department: .....

Contact telephone number:.....

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

Local authority reference:.....

Number of pages: .....

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

Magistrates' court:.....

Having considered the application, I (tick one):

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

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

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

Notes

.....

.....Reasons

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Unique Reference Number (URN)	

APPLICATION FOR NON-RIPA DIRECTED SURVEILLANCE AUTHORITY
(TO BE COMPLETED BY THE OFFICER MAKING THE APPLICATION/
LEAD OFFICER IN THE CASE)

Position	
Department	
Address	
Telephone Number	
Name of Applicant	
Email address	
Operation Name (if applicable)	
Date	

4. Authority Required From:
Head of Service/ YES/NO Service Manager or equivalent (delete as appropriate)
Head of Paid Service/ Chief Officer (Confidential Material Only) YES/NO

5. Background Information
a) Describe the purpose of the specific investigation/ operation.
b) Describe in detail the surveillance operation to be authorised, including any premises or vehicles which will be included in the surveillance or technical equipment (camera, binoculars, sound recorder, fixed cameras) that may be used for the surveillance. Give the expected duration of the surveillance and location of any such equipment. Where appropriate, a map can be attached to this application to denote the area within which the surveillance is to take place.
c) Outline the information expected to be obtained from this activity.

3. Particulars/ details (where known) of subject (s) against whom this surveillance is directed.	
• Name • Alias • DOB • Address • Any other relevant information	• Name • Alias • DOB • Address • Any other relevant information
4. Necessity	
Directed Covert Surveillance can only be undertaken by the Council where the surveillance is **necessary for the purpose of preventing or detecting crime or preventing disorder** (Section 28(3)(b)). Explain <u>why</u> this surveillance is necessary on this ground giving specific details of the alleged crime and/or disorder.	
5. Proportionality	
Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? Why is this intrusion outweighed by the need for surveillance in operational terms? Can the evidence be obtained by any other less intrusive means? If not, why not?	
6. Collateral Intrusion	
Supply details of any potential collateral intrusion and why that intrusion is unavoidable.	
What steps do you intend to take to minimise this collateral intrusion?	
7. Confidentiality	
Assess the likelihood of acquiring confidential material, such as • Legal Privilege • Confidential Personal Information • Spiritual Counselling • Confidential Journalistic Material	
8. Other operations	
Are there any other operations/investigations being undertaken or planned by other departments/ public authorities e.g. Police which could impact on the deployment of surveillance or compromise the proposed activity?	
9. Applicant	

Name		Position	
Signature		Date	