| Internal Ref: | NELC RIPA 01 APP1 |
| --- | --- |
| Review date | Not appropriate |
| Version No. | V01.5 |



# **Detailed guidance on completion of a RIPA application (directed surveillance)**

The officer must provide their name, work address, department and contact details.

The applicant must complete all relevant parts of the form as fully as possible to justify the use of directed surveillance paying particular attention to the individual circumstances of each application. Guidance on the completion of each section is detailed below and an aide-memoir is also available.

**Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers Act 200[[1]](#footnote-1)**

Provide the job title of the Authorising Officer. The list of authorising officers is available on the intranet. If there is any doubt as to whether an officer is authorised, contact Legal Services for advice.

# **Describe the purpose of the specific operation or investigation**

This section is used to provide the Authorising Officer with details of the investigation/operation.

The application form must hold sufficient information to justify the authorisation without reference to other documents. Therefore, it is essential that details of the reason for the investigation/operation are included in this part.

Include details of the original reason for starting the investigation/operation and a summary of the present position leading to the request.

# **Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment**

This section requires the applicant to provide the full extent of surveillance to be conducted. It is essential that the surveillance is described in detail as the Authorising Officer cannot authorise any activity that is not included. For example, if authorisation is requested to conduct static surveillance, even if the Authorising Officer believes that mobile surveillance would also be justified, they cannot authorise it as it was not in the application.

Therefore, it is good practice to conduct a reconnaissance visit to the area where surveillance will take place to ensure that the type of activity described is actually possible. For example, if it is intended to use camera equipment, can the camera be located effectively to achieve the desired result? Not only will this inform the type of activity to be undertaken, but it is also useful as part of a health and safety risk assessment and in providing a proper assessment of collateral intrusion.

Include the following information (if appropriate) in this section:

* The place(s) where surveillance is to take place;
* The duration of the surveillance or times between which it is intended to conduct the surveillance;
* The number of officers that are to be involved (in joint operations this should include the number of officers from other organisations covered by this authorisation)
* How those officers will be deployed (for example, static surveillance, mobile surveillance, etc.)
* Whether vehicles will be used and if so in what way;
* Whether it is intended to use other equipment (for example, cameras, binoculars, etc.);
* How surveillance will be recorded (for example, contemporaneous notes, video recording, still photographs);
* The location of surveillance equipment (vehicles, cameras, etc.)

This list is not exhaustive.

# **The identities, where known, of those to be subject of the directed surveillance**

In this section include details of all persons that will be subject to the surveillance. Provide names, addresses and dates of birth where known. If unknown specify the number of subjects and any other identifying features such as approximate ages or descriptions if held.

# **Explain the information that it is desired to obtain as a result of the directed surveillance**

Provide details of the purpose of the directed surveillance. Explain what information you believe conducting such surveillance will provide to further the investigation.

Do NOT use phrases such as ‘to prove an offence has been committed.’ This implies that your assessment is not objective as you have presumed the subject is guilty and therefore, it could be open to challenge under article 6 *Right to a fair trial.*

It is therefore, essential that the information provided is objective.

Example:

An allegation of benefit fraud is received alleging that a person is working. We wish to use directed surveillance to obtain the following information: ‘To establish whether or not the subject is working and if so where and for whom.’

This is an objective assessment of the information that we wish to obtain. It does not make any assumptions as to whether or not any offence has been committed.

However, the following would be a subjective assessment: ‘To establish where the subject is working.’ This is subjective because we have made an assumption that the subject is working and therefore, guilty based on the allegation

# **Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA.**

An authorisation under RIPA can only be given if the surveillance operation is for the purpose of preventing or detecting crime.

Where surveillance falls outside of these grounds it does not mean that the surveillance is unlawful, but that the protection afforded by RIPA does not apply. In such circumstances these forms will still be used and will be treated as a “Non-RIPA” authorisation. This means the same scrutiny and attention to detail should be applied in ensuring that a breach of human rights does not occur. The same process should be followed. If in doubt the authorising officer should seek legal advice.

# **Explain why this directed surveillance is necessary on the grounds you have identified**

Once it has been identified that directed surveillance is necessary for the purpose of preventing or detecting crime or of preventing disorder, use this section to explain why the surveillance is necessary in this particular investigation/operation.

To satisfy the test of necessity, it has to be shown that the information sought will progress the operation/investigation. For example:

Using the previous benefit fraud example, the directed surveillance would progress the investigation by providing evidence of whether or not the person was working and where. If they were working and his place of work identified we could then obtain details of his employment. If they were not working, it may mean that the investigation could be closed. These details should be included in this section

# **Supply details of any potential collateral intrusion and why the intrusion is unavoidable.**

Collateral Intrusion is the intrusion into or interference with the privacy of persons other than the subject(s) of the investigation/operation. The Authorising Officer will have regard to the potential for collateral intrusion when considering the proportionality of directed surveillance and therefore, the fullest details must be included.

There will always be the potential for collateral intrusion when undertaking directed surveillance. Any member of the public going about their private business may be subject to collateral intrusion if they are observed during the surveillance. Likewise, other members of the subject(s) family may be subject of collateral intrusion if surveillance is conducted on a residential property.

Therefore, this section of the application must include an assessment of the risk and a plan to reduce the risk to an acceptable level. If the risk cannot be reduced to a level proportionate to the offence being investigated the Authorising Officer must reject the application.

The risks of collateral intrusion will be unique to each investigation/operation depending on the surveillance as described at part 3 of the application form. The risks may include:

* The area in which surveillance is intended to be conducted. The more densely populated the area (for example a housing estate), or busier the area (for example a main road) the greater the risk of collateral intrusion;
* The time of day the surveillance operation is intended to take place. For example, a works entrance may be busier at clocking on time than any other time, thus increasing the risk of collateral intrusion at this time;
* The amount of time it is intended to conduct the surveillance operation. In general, the greater the amount of time, the greater the risk of collateral intrusion;
* The specific location(s) under surveillance. For example, where a residential property is under surveillance, there is a risk of collateral intrusion into other members of the household who may be observed entering and leaving the property;
* Where cameras are used, consider the line of sight. Is there an increased risk from the area the camera(s) cover(s)?
* This list is not exhaustive and the risks in each individual case may include some or all of the above.

In addition, special attention should be paid where collateral intrusion is likely to be sensitive. Examples include:

* Where surveillance is likely to interfere with the privacy of children. This may be where there is a school in the vicinity, or where it is known that there are children in a property under surveillance;
* Where surveillance is conducted on premises used by lawyers or for any form of medical or professional counselling or therapy;
* Where the subject of surveillance might reasonably expect a high degree of privacy, for example at home. Whilst it is lawful to undertake directed surveillance in a public place, this does not extend into the subjects house (This is intrusive surveillance and Local Authorities are not empowered to undertake such activities). Therefore, care must be taken to ensure no intrusive surveillance is conducted.
* Where similar activities are being undertaken by other public authorities that could impact on the deployment of surveillance.

Having identified the risks, there must be a plan to minimise them. This may include restricting times/duration of surveillance, amending the positioning of static surveillance, reducing the number of officers/vehicles deployed. Include in the plan how collateral intrusion will be recorded (if at all) and for what purpose.

The Authorising Officer must be informed if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

# **Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?**

The use of directed surveillance will not be proportionate unless it can be shown that:

* there are no less intrusive ways of obtaining the information;
* it is not excessive in what it seeks to achieve, and;
* the intrusion into the subject’s privacy (and that of others) is outweighed by the need to conduct the surveillance.

Use this section to provide details of all less intrusive means that have been employed to obtain the information and the result of those enquiries. Where other less intrusive lines of enquiry have not been followed, explain why. This may also include approaching the suspect(s).

Provide details of the extent of the potential offence. Include details of the seriousness of the offence and the prevalence of the type of offence in the area. If known, indicate the potential loss to the Authority or individuals as a result of the offence and the amount of time over which it has been committed (if relevant).

The intrusion into the privacy of others should have been justified in section 8 on collateral intrusion, therefore, in this section provide details to justify the intrusion into the subject(s) private life. In general terms if the first two points can be justified this will provide justification for the intrusion.

# **Confidential information**

An explanation of confidential material can be found in part two of this guidance.

Confidential information should not be confused with ‘private information’. The obtaining of private information on a subject is one of the considerations when deciding whether RIPA authorisation is required but should be given its normal meaning of information about a person that is not public information.

RIPA does not provide any special protection for confidential material. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under this code. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to special authorisation.

In general, any application for an authorisation that is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

Only the Head of Paid Service (or in their absence the person acting as Head of Paid Service) are empowered to authorise requests for obtaining confidential information.

The following general principles apply to confidential material acquired under authorisations:

* Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Legal Services before further dissemination takes place;
* Confidential material should not be retained or copied unless it is necessary for a specified purpose;
* Confidential material should be disseminated only where an appropriate officer (having sought advice from the Legal Services) is satisfied that it is necessary for a specific purpose;
* The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.
* Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose

# **Authorising officers considerations**

No officer shall grant an authorisation for the carrying out of directed surveillance unless they believe that the directed surveillance is both necessary and proportionate to the investigation/operation being undertaken and that the surveillance is required for the purposes of preventing or detecting crime or preventing disorder.

It is the Authorising Officers responsibility to clearly identify the activity to be undertaken and to demonstrate that they have fully considered the necessity and proportionality of the activity. It is not sufficient for the Authorising officer to simply endorse the application.

# **Authorising Officers Statement**

In this section, the Authorising Officer must detail **who** the surveillance is directed against, **when** the surveillance will occur, **where** the surveillance will take place and **how** it will be achieved, for example, what equipment will be used, how many officers will be deployed.

Only activities included in the Authorising Officer’s statement will be covered by RIPA. Therefore, it is essential that the Authorising Officer’s statement covers all aspects of the activity to be undertaken. However, the Authorising Officer cannot authorise any activity that has not been requested by the applicant. Therefore, it is important that the applicant considers the full extent of the activity they require when completing part 3 of the form.

Where the Authorising officer believes that an activity not requested is appropriate, they should discuss this with the applicant with a view to the application being amended to include the additional activity.

# **Explain why you believe the directed surveillance is necessary. Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out.**

In this section the Authorising Officer should set out **why** they are satisfied that the surveillance is both necessary and proportionate to what it seeks to achieve. Where the applicant has provided insufficient information to justify the intrusion, the Authorising officer should consider returning the application for the information to be included.

Regardless of whether the application is authorised or refused, the Authorising Officer must provide written justification for their decision. It is not sufficient to simply state that the surveillance is (or is not) necessary and proportionate. The reasons why must be included.

# **Additional considerations**

In addition to the considerations on necessity, proportionality, collateral intrusion and confidential material made as part of an application, the applicant and Authorising Officer must have regard to any spiritual counselling, as detailed below:

* No operations should be undertaken in circumstances where investigators believe that surveillance will lead to them intrude on spiritual counselling between a Minister and a member of his/her faith. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.
1. For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards. [↑](#footnote-ref-1)