



CARDIFF

---

CAERDYDD

---

**OPERATIONAL POLICY AND GUIDANCE ON THE USE OF DIRECTED  
SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS  
ACT 2000**

**May 2013**

# OPERATIONAL POLICY AND GUIDANCE ON DIRECTED COVERT SURVEILLANCE AND AUTHORISATION UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000, as amended (RIPA)

## 1. What is covert surveillance?

RIPA defines surveillance as including

- *monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;*
- *recording anything monitored, observed or listened to in the course of surveillance; and*
- *surveillance by or with the assistance of a surveillance device.*

Covert surveillance is surveillance, carried out so that the people being observed, or listened to, or monitored, are unaware that it is, or may be taking place.

## 2. When might the Council undertake covert surveillance?

The Council is involved in every day functions of law enforcement. This is mainly done in an overt manner. However, there will be occasions when Council officers undertake their duties in a covert manner. For example Trading Standards might covertly observe traders to ensure compliance with legal requirements.

RIPA provides a framework for regulating the use of those investigatory powers ensuring that any covert surveillance activities are consistent with the duties imposed upon public authorities by the Human Rights Act. The Act provides that covert surveillance will be lawful if an authorisation has been properly issued and a person acts in accordance with that authorisation. This is important because if the Council is involved in any proceedings before the Court the Council will be able to show that it has acted lawfully and that it has gathered evidence properly.

The Council has to be satisfied that:

- *Any surveillance is undertaken in connection with a statutory function with which the Council is charged.*
- *That such interference can be justified legally.*
- *The surveillance is properly authorised in accordance with this policy and consequently provides a basis for justifying any interference with a person's Human Rights.*

### 3. What is Directed Surveillance?

Directed Surveillance is covert surveillance undertaken:

- for the purposes of a specific investigation or a specific operation;
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not 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 this Part to be sought for the carrying out of the surveillance

### 4. When can Council Officers use Directed Surveillance?

Council officers can use directed surveillance to prevent and/or detect crime, where the crime under investigation carries a custodial sentence of 6 months or more and also for the investigation of offences relating to the illegal sale of alcohol or tobacco to minors. Such offences are considered to meet the “crime threshold”. If these conditions are not satisfied, the Council cannot conduct surveillance under RIPA.

If the proposed surveillance activity takes place in residential premises or in a private vehicle and involves the presence of a person or surveillance device in the premises or vehicle, such surveillance is then referred to as Intrusive Surveillance. No officer of the Council is authorised to approve an authorisation under RIPA for Intrusive Surveillance.

The fact that covert surveillance may not be authorised under RIPA does not necessarily mean that the actions proposed cannot lawfully be undertaken, and the advice of an authorising officer should be sought before any surveillance is contemplated. (*reference Case No: IPT/11/129/CH; IPT/11/133/CH & IPT/12/72/CH*)

The changes introduced by SI. 2012:1500 and Sections 37 and 38 of the Protection of Freedoms Act 2012 mean that judicial approval is required before any covert surveillance can be carried out.

***Throughout this guide the term authorisation refers to an internal consent to take the process forward. The term approval is a judicial consent to make the application lawful.***

## 5. How is an application for an authorisation made?

An application for authorisation for Directed Surveillance must be in writing and use the application form held on the Intranet ([4.c.199a](#)). It will contain:

- The action to be authorised;
- The identities, where known, of those to be the subject of directed surveillance;
- An account of the investigation or operation;
- An explanation of the covert techniques that will be used, *N.B. the use of CCTV (see section 10 below)*
- Confirmation that the action proposed is intended to prevent or detect crime
- A statement outlining why directed surveillance is considered to be proportionate to what it seeks to achieve;
- An explanation of the information which it is desired to obtain as a result of the authorisation;
- An assessment of the potential for collateral intrusion, that is to say, interference with the privacy of persons other than the subjects of the surveillance, and an assessment of the risk of such intrusion or interference;
- An assessment of the likelihood of acquiring any confidential material and how that will be treated
- Where authorisation is sought urgently, the reasons why the case is considered to be urgent.

## 6. Approving the use of Directed Surveillance?

The Act, as amended, identifies Authorising Officers as Director, Head of Service, Service manager or equivalent In Cardiff; this will be construed as a member of the senior management team. However the following are those who by virtue of their function will ordinarily and primarily act as Authorising Officers:

*Head of Regulatory and Supporting Services*

*Director Environment*

*Assistant Director Environment*

*Director, Communities, Housing and Customer Services*

*The Chief Executive*

Ideally the Authorising Officer should not be responsible for authorising surveillance within their own direct sphere of activity, i.e. those operations or investigations in which they are directly involved or for which they have direct responsibility.

## 7. What will the Authorising Officer have to consider in processing an authorisation?

Authorising Officers, and officers authorised to conduct directed surveillance must be familiar with the requirements of any relevant Codes of Practice issued by the Home Office.

An authorisation can only be considered if the proposed covert activity aims to prevent or detect crime. The proposed activity should relate to a specific purpose that is part of the Councils statutory, or core, function. The concept of statutory or core functions of public authorities is not set out in the Act, but the decision in IPT [IPT/03/32/H provides guidance](#). It is not easy to define the concept in general terms or to propound a general test for distinguishing between the core functions and the ordinary functions of public authorities. However, such a distinction is implicitly recognised in RIPA by the nature of the grounds on which the Council may be authorised to conduct directed surveillance under RIPA, i.e. to prevent or detect crime.

To consent to an authorisation, the Authorising Officer must be satisfied that the proposed surveillance is **necessary** for the purpose of preventing and detecting crime that meets the crime threshold.

The Authorising Officer must also believe that the proposed surveillance is **proportionate** to what it seeks to achieve and that any potential for **collateral intrusion** and the likelihood of acquiring any **confidential material** is reduced to a minimum. Reference must be made to the statutory code of practice on covert surveillance.

There must be a record of whether approval was given or refused, by whom and the time and date. ([form 4.c.199b](#)) Service areas may use a range of techniques and equipment to undertake covert surveillance. Service areas must ensure that the use of covert equipment is managed appropriately and the technical capacity of such equipment is made known to the Authorising Officer when it is deployed for covert purposes.

*N.B. The safety of the public and council staff must override all other considerations. Authorising Officers must consider violence at work, fatigue, lone working, etc. Where appropriate the Authorising Officer should call for a risk assessment to be conducted before granting the authorisation.*

## 8. What does the term “necessary” mean?

RIPA provides a framework for ensuring that any surveillance activities do not infringe the Human rights of the individual. In considering whether to grant an authorisation, the authorising officer must consider whether the proposed conduct is *necessary*.

The fact that a crime may have been, or is about to have be committed, does not automatically mean that covert surveillance is necessary. There must be a pressing need for a covert operation to be undertaken and there must be a clear reason for the covert activity. Council Officers should not seek to obtain information through covert means that is not needed for an investigation. It might be useful and very interesting to acquire information about a particular individual, but if it is not strictly necessary to have it then officers should not seek to obtain it. Officers need to show necessity in each case.

## 9. What does the term “proportionate” mean?

Proportionality is a very important concept. At its simplest, proportionality is about balancing the human rights of the individual against the need to undertake covert surveillance to further an investigation. An authority should not be granted upon grounds of the seriousness of the offence alone.

Any interference with a person’s rights must be appropriate and justifiable. An Authorising Officer must consider a number of issues in deciding if a proposed course of action is proportionate. Most importantly is the belief that the Council has relevant and sufficient reason for interfering with an individual’s right to respect for family and private life.

If an Authorising Officer decides that the required information needs to be acquired in a covert manner and that it cannot reasonably be acquired by other means that would involve less, or no, invasion of privacy; that decision must be carefully documented and show how the Council has

- Balanced the size and scope of the operation against the gravity and extent of the perceived mischief,
- Determined that the methods to be adopted will cause the least possible intrusion on the target and others,
- Determined that the activity is an appropriate use of the legislation and the only reasonable of obtaining the necessary result,
- Examined other methods of achieving the requisite information and why they were not used

Interference will not be justified if the means used to achieve the aim are excessive in all the circumstances. Thus where surveillance is proposed, the covert action must be designed to do no more than meet the objective in question; it must not be unfair or arbitrary; and the impact on the individual or group of people concerned must not be too severe.

Every case must be considered on its merits; what is proportional in some circumstances will not be proportional in others. Authorising Officers need to ensure that an applicant has considered other ways to obtain the required information, or evidence, such as use of third party information powers, the Internet, and other sources.

#### **10. What does the term “collateral intrusion” mean?**

Collateral intrusion occurs when officers obtain information about people unconnected with the investigation. Authorising Officers must consider the likelihood and extent of collateral intrusion when considering any application and ensure that applicants have planned to minimise collateral intrusion. Situations where collateral intrusion can occur include where:

- Observing business premises may result in watching unconnected people come and go
- During an operation observing or overhearing other conversations that are not relevant to the investigation and impact upon the privacy of others.

It is important to understand that what is done in public does not automatically cease to be private. Members of the public are aware that public authorities use CCTV in an overt manner to prevent crime. Where such systems are used for a specific covert purpose, the covert operation shall not start until the owner/operator of the CCTV system has been shown the Authorisation for the covert action and has been briefed on the parameters of the covert action.

#### **11. What does the term “confidential material” mean?**

Confidential material is anything:

- That is subject to legal privilege, for example communications between a legal adviser and his/her client.
- That is confidential personal information, for example information about a person’s health or spiritual counselling or other assistance given or to be given to him or her.
- That is confidential journalistic material (this includes related communications), that is, material obtained or acquired for the purposes of journalism and subject to an undertaking to hold in confidence.

If there is a likelihood that confidential material will be obtained as a result of covert surveillance, the authorisation can only be considered by the Chief Executive, or in his absence, the County Solicitor.

## 12. Applying for judicial approval

Following the issue of an authorisation by an AO, the applicant must contact the Magistrates Court to arrange a hearing. All relevant paperwork should be available for the Court to examine and officers should complete form [4.c.199d](#) – the judicial approval form. A magistrate will make one of the following decisions:

- **Approve the application**

If the application is approved, the magistrate will issue form [4.c.199e](#). The grant of the application will then take effect and the Council is now able to use the covert technique for that particular case.

- **Refuse to approve application**

The RIPA authorisation or notice will not take effect and the Council cannot use the technique in that case.

If an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without going through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those steps have been taken.

- **Refuse to approve the grant and quash the authorisation**

This applies where a magistrates' court refuses to approve the grant and decides to quash the original authorisation or notice. The court must not exercise its power to quash that authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

## 13. How long will an approval last?

The written approval will normally cease to have effect (unless renewed) at the end of a period of 3 months beginning with the date on which it took effect.



## 14. Reviewing authorisations/approvals

It is the duty of Authorised Officers to review periodically all the circumstances relating to an application. Such reviews should take place, at least, on a monthly basis. Any notes relating to the review must be recorded on the Review form held on the Intranet. Reviews should be more frequent where there may be collateral surveillance on persons other than those who are the subject of surveillance. Reviews must be recorded using form [4.c.233](#)

If a decision is taken to cease surveillance, an instruction must be given to those involved in the operation to stop listening, watching, or recording the activities of the subject. The date on which that instruction is given should also be recorded.

N.B. Magistrates **do not** consider internal reviews

## 15. Renewing Authorisations

If an applicant wishes to continue a covert surveillance exercise for the same purpose for which it was given, then he/she may apply to renew it in writing for a further period beginning with the day when the authorisation would have expired but for the renewal.

Any request for a renewal of an authorisation should be recorded using the Renewal form [4.c.200](#) on the Intranet outlining:

- Whether this is the first renewal, or on how many occasions it has been renewed;
- The same information as outlined for an original application;
- Details of any significant difference in the information given in the previous authorisation;
- The reasons why it is necessary to continue with the surveillance;
- The content and value to the investigation or operation of the information so far obtained by the surveillance;
- An estimate of the length of time the surveillance will continue to be necessary.

Any renewal application will follow a similar process through the Magistrates.

## 16. Cancelling an authorisation

The Authorising Officer who granted or last reviewed/renewed the authorisation must cancel it if he/she is satisfied that the Directed Surveillance no longer meets the criteria for authorisation. If that Authorising Officer is unavailable, another Authorising Officer must undertake that role and ensure that surveillance ceases. Cancellation must be recorded using form [4.c.201](#)

N.B. Magistrates **do not** consider cancellations

## 17. What records must be kept?

The following records must be kept:

- A copy of the application for authorisation.(4.c.199a)
- A copy of the authorisation.(4.c.199b)
- A copy of the judicial application (4.c.199d)
- A copy of the judicial approval (4.c.199e)
- A record of the period over which the surveillance is taking or has taken place (including any significant suspensions of coverage).
- A record of the result of periodic reviews of the authorisation. (4.c.233)
- A copy of any renewal of authorisation, together with the supporting documentation when the renewal was requested. (4.c.200)
- A copy of the cancellation of the authorisation (4.c.201)

## 18. Who keeps the record?

The County Solicitor acts as the SRO and will maintain a central register of records. The Central Register is held electronically and access is restricted. Authorising Officers are responsible for ensuring that they provide timely information to enable the Central register to reflect all current activities and to avoid duplication of resources.

The role of the Senior Responsible Officer is to oversee the competence of Authorising Officers and the processes in use. Whilst legislation does not preclude the SRO acting as an authorising officer, it is unlikely given the lack of objectivity if the SRO oversees his/her own authorisations.

## 19. Who is responsible for overseeing compliance with RIPA?

Under the Act, the Chief Surveillance Commissioner and Surveillance Commissioners together with their Assistants have been appointed to provide independent oversight of the use of the powers contained in Part 2 of the Act. They will inspect the Council from time to time to ensure that the Council is complying with the Act. In addition, the Act establishes an independent tribunal. This tribunal has full powers to investigate and decide any case where a person complains about the conduct of the Council in exercising its powers carrying out surveillance. This policy also forms part of the Councils quality protocols and as such is liable to scrutiny. All officers involved in activities affected by this policy must observe the guidance contained in this document.

## 20. What reference documents are there?

The Council and those persons acting under Part 2 of the Act must have regard to the Codes of Practice issued under the Act. Each Authorised Officer will have copies of these codes. In addition, the Council has prepared 4 specific forms for use by officers in relation to Directed Surveillance. These forms are available on the Intranet site.

Where fraud or corruption is suspected, then regard should be had to the Council's Anti-fraud and Anti-corruption strategy.

1.CM.121	Issue 4	May 2013	Process Owner: City and County Solicitor	Authorised: Council	Page 10 of 10
----------	---------	----------	--	---------------------	---------------