

Legally intruding into people's privacy

1. Introduction

This policy sets out the County Council's position regarding the Regulation of Investigatory Powers Act 2000 (RIPA).

At first glance RIPA appears to have little application to the County Council as it largely relates to police surveillance and investigation activity. However, it is relevant not only to the specialist investigatory sections of the County Council such as the Trading Standards team but also it is of potential relevance generally to the work of the Council where investigations could occur.

RIPA provides useful tools to aid investigating whilst requiring that the correct procedures are followed in authorising any such investigations. To be fully understood RIPA has to be seen in the wider legal context of human rights.

1.1. Human Rights

The County Council is required to act in accordance with the provisions of the Human Rights Act 1998 which gives effect in domestic law to some of the terms of the European Convention on Human Rights.

Under section 6 of the Human Rights Act it is unlawful for the County Council to act in a manner that is incompatible with European Convention rights such as the right to respect for a persons private and family life, their home or correspondence. This particular right is contained in Article 8 of the Convention and it prevents interference by a public authority such as the County Council except in certain limited circumstances. Such interference can be acceptable if it is "in accordance with the law". RIPA provides such a legal means of interfering with an individual's privacy providing the necessary considerations take place and the appropriate authorisations are given.

2. DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

The two principal activities that make the Act applicable to the County Council are the use of "**Directed Surveillance**" and the use of "**Covert Human Intelligence Sources**" or CHIS.

In lay terms these mean:

- **Directed Surveillance** – specifically focussing attention on an individual under suspicion to try and establish criminal behaviour.
- **Sources** – someone who provides information in more than one contact to the County Council and for whom there is some inherent personal risk.

3. APPLICATION OF THE ACT

RIPA therefore has the potential to apply across the County Council. The current custom and practice in a department or team may be to conduct all enquiries in an open manner such that RIPA is not engaged. However because it is possible that situations may arise where the best means of obtaining information is by covert means it is important that all departments are aware of the procedures to follow under RIPA and the potential benefits such working might bring. The circumstances where RIPA might be applicable across the Authority could include:-

- Officers might find local CCTV networks useful in tracing particular truants
- Officers might wish to check secretly whether rights of way are being blocked or might be considering enforcing a planning matter and need secret surveillance to prove their case

4. AUTHORISATIONS

The use of Directed Surveillance or CHIS to pursue a particular line of enquiry must under RIPA, be properly authorised. This involves the intrusion into someone's privacy or the risk a CHIS takes being considered by someone other than the officer wishing to take the action. Ultimately it ensures that any evidence resulting from the operation has been lawfully obtained. It also limits the level of any intrusion or risk.

Each Department will have in place **Authorising Officers** at appropriate senior levels, who are at least one level removed from the investigation but preferably at second tier Officer level who will be trained to enable them efficiently to fulfil their duties under RIPA.

A central record of authorisations will be held by the RIPA Act nominated Monitoring Officer in Legal Services.

5. NECESSITY AND PROPORTIONALITY

The principal concepts that those seeking authority and those considering such authorisations must consider and address are whether the surveillance or source are **necessary** to the particular operation or enquiry and whether the surveillance or sourcing suggested is **proportionate**. This in lay terms means:

- **Necessity** – where the information sought could be found in another means such as walking past and observing an address or asking the employee concerned, the use of surveillance will not be “necessary”. Or put another way, can the information be obtained openly? If the answer is yes then the surveillance is not “necessary”.
- **Proportionality** – this entails asking what the least intrusive form of the surveillance or sourcing is that would result in the information sought being obtained. For example, the use of CCTV of a part-time officer suspected of theft would not be proportional if it was authorised for a whole week.

6. PROCEDURE

The County Council is a Relevant Authority for the purposes of Section 28 (Authorisation of Directed Surveillance) and Section 29 (Authorisation of Covert Human Intelligence Sources).

6.1. Directed Surveillance

Section 26(2) defines surveillance as being directed if it is covert but not intrusive and is undertaken:

- a) for the purposes of a specific investigation or a specific operation;
- b) 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
- c) 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 Part ii of the Act to be sought for the carrying out of the surveillance.

NOTES:

- **Surveillance** is defined at Section 48(6) of the Act as monitoring, observing or listening to persons, their movements, conversations, activities or communications.
- **Covert** has a dictionary definition including secret which in this context means unknown by the person under suspicion.
- **Intrusive surveillance** means at somebody’s house or in their car.
- **Monitoring** has a dictionary definition which includes the idea of watching but also includes examining and scrutinising.
- **Private information** in relation to a person includes any information relating to his/her private or family life. (Section 26(10)).

6.2. Authorisation of Directed Surveillance (Section 28)

The details of which officers can authorise directed surveillance in each Department are set out in Schedule 1.

Form DS1 (Part ii application for Authority for Directed Surveillance) will be filled in by the investigating officer and submitted to an Authorising Officer.

If the Authorising Officer agrees to authorise the directed surveillance, after considering the requirements of Section 28 and the guidance in the Code of Practice, then she/he will fill in and issue Form DS2 (Authority for Directed Surveillance Operation).

Form DS1 and DS2 should be attached to each other.

In urgent cases authorisation may be given orally (usually by telephone) and the investigating officer should record this on Form DS3 (Record of Urgent Authorisation) which is on the back of Form DS2, as soon as is reasonably practicable. This form should be endorsed by the authorising officer as soon as reasonably practicable.

All written authorisations will continue until such time as they are formally withdrawn. Regular reviews must be undertaken to avoid authorisations running on unnecessarily (these will be between 1 and 3 months depending on the activity authorised and the particular facts of each case). The authorising officer who reviews the authorisation must consider again the issues of necessity and proportionality.

Urgent authorisation will only be given for 72 hours beginning with the time when the authorisation was granted and will then be formally withdrawn unless renewed.

Form DS4 (supplementary form for renewals) will be submitted by the investigations officer to apply for an authorisation renewal.

Form DS5 (Renewal of authority for directed surveillance operation) will be completed and issued by the authorising officer if he is satisfied that the criteria for authorisation is still met.

The officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the directed surveillance no longer meets the criteria for authorisation using Form DS6 (Cancellation of Directed Surveillance).

Copies of any Forms DS1 to DS6 should be sent to the RIPA nominated Monitoring Officer within 5 working days.

It will be the responsibility of the Monitoring Officer to maintain a central record of all authorisations for directed surveillance.

6.3. Covert Human Intelligence Sources

Section (26(8) defines a person as being a covert human intelligence source if

—

- a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling

within paragraph (b) or (c);

- b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- c) he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

NOTES:

- A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that one party is unaware of its purpose. For the definition of “covert purpose” see Section 26(9(b)).
- A member of the public volunteering information to us would not at that stage be a covert human intelligence source but will become so as soon as we encourage him/her to act as one in gathering further information through a relationship that fits the Section 26(8) definition.

6.4. Authorisation of covert human intelligence sources (Section 29)

The details of which officers can authorise the use of covert human intelligence sources in each Department are set out in Schedule 1.

Form CHIS1 (Part ii application for authorisation of the use or conduct of a covert human intelligence source) will be filled in by the investigating officer and submitted to an authorising officer.

If the authorising officer agrees to authorise the use or conduct of a covert human intelligence source, after considering the requirements of Section 92 and the guidance in the Code of Practice, then he will fill in an issue Form CHIS 2 (Authorisation of the use of conduct of a covert human intelligence source).

Forms CHIS1 and 2 should be attached to each other.

In urgent cases authorisation may be given orally (usually by telephone) and the investigating officer should record this on Form CHIS3 (Record of Urgent Authorisation) which is on the back of Form CHIS2, as soon as is reasonably practicable. This form should be endorsed by the authorising officer as soon as reasonably practicable later. The Authorising Officer must also complete a Source Identify form, ensuring that the Operation Reference Number corresponds with that on the CHIS1.

6.5. Juvenile Sources

The use of juveniles as covert human intelligence sources is to be authorised only by the officers listed in Schedule 1 and not to a delegated officer and only after consideration has been given to the Requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 and the Code of Practice.

6.6. Vulnerable individuals as sources

Vulnerable individuals, such as the mentally impaired, should only be authorised to act as a source in the most exceptional circumstances and such authorisation will only be given by the officers listed in Schedule 1 and not to a delegated officer.

6.7. Duration

All written authorisations will continue until such time as they are formally withdrawn. Regular reviews must be undertaken to avoid authorisations running on unnecessarily (these will be between 1 and 3 months depending on the activity authorised and the particular facts of each case). Juvenile sources will be reviewed no later than 28 days after the granting of an authorisation. The authorising officer who reviews an authorisation must consider again the issues of necessity and proportionality.

Urgent authorisation will only be given 72 hours beginning with the time when the authorisation was granted and will then be formally withdrawn unless renewed.

Form CHIS4 (supplementary form for renewal) will be submitted by the investigatory officer to apply for an authorisation renewal.

Before an Authorising Officer renews an authorisation, he must be satisfied that a review has been carried out of the use made of the source during the period authorised, the tasks given to the source and the information obtained from the use or conduct of the source. The key issue to consider is the risk involved in the operation to the source.

If the authorising officer is satisfied that the criteria for the initial authorisation continue to be met, he/she may renew the authorisation by completing and issuing form CHIS5 (Renewal of authorisation for use or conduct of a covert human intelligence source).

The officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the use or conduct of the source no longer satisfies the criteria or that the arrangements for oversight and management of the source are no longer in place. (Form CHIS6 (Cancellation of the use or conduct of a covert human intelligence source)).

6.8. Management of Sources

Every source should have a designated handler which will normally be the investigating officer applying for the authorisation.

“Handler” means the person referred to in Section 29(5)(a) of the Act who will have day to day responsibility for:-

- dealing with the source on our behalf;

- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

Also every source should have a designated controller which would normally be the line manager of the investigating officer.

“Controller” means the officer referred to in Section 29(5)(b) of the Act, responsible for the general oversight of the use of the source.

6.9. Tasking

Tasking is the assignment given to the source by the handler or controller, asking him/her to obtain information, or to otherwise take an action leading to the obtaining of information.

When unforeseen actions or undertakings occur when a handler meets a source, or the source meets the target of an investigation, any such actions or undertakings must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient, a new authorisation should be obtained before any further such action is carried out.

Copies of any Forms CHIS1 to CHIS6 should be sent to the Monitoring Officer within 5 working days. The source Identity form is to be retained by the Investigating Officer and all contact with the source must be recorded. This should be sent to the Monitoring Officer only when the authorisation of the source in relation to a specified task ceases. It will be the responsibility of the Monitoring Officer to maintain a register of all authorisations granted for the retaining of covert human intelligence sources.

6.10. Security and Welfare

Before authorising the use or conduct of a course, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known to the target or those involved in the target activity. The ongoing security and welfare of the source, after the end or cancellation of the authorisation, should also be considered at the outset.

The handler is responsible for bringing to the controller's attention any concerns about the personal circumstances of the source, insofar as they might affect:-

- the validity of the risk assessment
- the proper conduct of the source operation; and
- the safety and welfare of the source.

Any such concerns must be brought to the attention of the authorising officer by the controller and a decision taken on whether or not to allow the authorisation to continue.

NOTE: the Authorising Officer might be the controller.

6.11. Record Keeping

Records must be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source.

The records should contain the particulars as set out in paragraph 3.13 and 3.14 of the Code of Practice “The Use of Covert Human Intelligence Sources”, and these should be made and updated by the investigating officer and copies of the records or updates must be sent to Monitoring Officer within 5 working days.

7. CONFIDENTIAL MATERIAL (Relevant to Directed Surveillance and the Use of Covert Human Intelligence Sources)

“Confidential Material” has the same meaning as it is given in Sections 98-100 of the Police Act 1997

It consists of:-

- matters subject to legal privilege – this can include situation where there is litigation taking place involving legal advice and also simply where a solicitor-client relationship exists for the purpose of obtaining advice or assistance in relation to rights and liabilities;
- confidential personal information – this will include physical and mental health information held by healthcare professionals and spiritual counselling information held by Ministers of religion;
- confidential journalistic material – this is information obtained for journalistic purposes subject to an undertaking that it will be held in confidence.

For further definitions refer to the Codes of Practice.

Where any authorisation is likely to result in the acquisition of or knowledge of confidential material, the authorisation should only be considered by those authorised officers actually listed in Schedule 1 and not by any other delegated officer.

The general principles applying to confidential material acquired under Part ii authorisation are:-

- those handling material from such operations should be alert to anything which 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 appropriate Authorising Officer. 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 Authorising Officer 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.

8. Maintenance of documents

All original forms or copies relating to Part II authorisation will be stored securely by the RIPA Nominated Monitoring Officer and kept for six years after the completion of an operation. After that period private disposal will be considered in consultation with the appropriate Authorisation Officer.

9. Comment

These instructions should be ready in conjunction with the published Codes of Practice copies of which are available on the Home Office Website at:

<http://security.homeoffice.gov.uk/news-and-publications1/ripa-forms/?version=1>

Copies of the Codes of Practice should be made readily available to all appropriate staff particularly all designated Authorising Officers and anyone to whom they may choose to delegate.

SCHEDULE 1

<u>Department</u>	<u>Authorising Officer</u>
Chief Executives	Assistant Chief Executive
Communities	Service Director Community Safety, Regeneration and Protection
Children and Young People	Service Director Social Care & Health
Adult Social Care and Health	Service Director Strategic Services
Resources	Service Director Finance & Trading