

SURREY COUNTY COUNCIL

POLICY & PROTOCOL

ON THE REGULATION OF INVESTIGATORY POWERS ACT

Including, Directed Surveillance, use of Covert Human Intelligence sources and the Acquisition of Communications Data

Scope

This Protocol applies to Covert Surveillance, Covert Human Intelligence Sources and the Acquisition of Communications Data, as defined in the Regulation of Investigatory Powers Act 2000, undertaken by officers of Surrey County Council.

Human Right Act principles and the Regulation of Investigatory Powers Act 2000

The Human Rights Act 1998 (HRA) came into force in October 2000. One of the principles enshrined in the Act is that everyone has the right to respect for their privacy and family life, home and correspondence and that there should be no interference by a public authority except in accordance with the law. The HRA recognises however that there are circumstances in a democratic society where it may be necessary for the State (which includes a range of public authorities of which Surrey County Council is one) to interfere with these rights. The Regulation of Investigatory Powers Act 2000 (RIPA) make provision for public authorities to carry out certain forms of surveillance and use covert human intelligence sources in the course of investigations but this can only be done in accordance with certain principles and for the following purposes:

- in the interest of national security, public safety or the economic well-being of the country
- the prevention of disorder or the prevention/detection of crime
- the protection of safety, health or 'public morals'
- the protection of the rights and freedoms of others (including the protection of the environment).

There is a duty on the Council to act in a way that is compatible with the individual's rights and failure to do so may enable a person to seek damages against the Council or to use our failure as a defence in any proceedings that we may bring against them.

RIPA only permits the Council to exercise powers for the purposes of preventing and detecting crime or preventing disorder.

To be able to justify any interference with the right to respect for an individual's privacy under the HRA, the Council needs to demonstrate that any interference is not only for one the prevention or detection of crime, but is also:

- **lawful**
- **necessary** for the purposes of the investigation and
- **proportionate** to what we want to achieve

Covert Surveillance

Covert surveillance is sometimes needed in an investigation, but is likely to be regarded as an intrusion into an individual's privacy and a possible breach of his/her human rights. RIPA has been enacted to protect public authorities from challenge on the basis of a breach of human rights. For this reason, the terms on which covert surveillance may lawfully be undertaken, and the Council protected, have been explicitly set out in the RIPA and a statutory Code of Practice. Consideration must also be given to the requirements of the Data Protection Act in respect of the subsequent retention, use and storage of data or information obtained.

Where covert surveillance is considered appropriate, it is necessary for it to be **formally authorised**. This applies whether the surveillance is to be undertaken by Council Officers or by an outside agency acting on the Council's behalf. Authorising officers will need to satisfy themselves that a defensible

case can be made for the covert surveillance activity. RIPA applies controls on “directed surveillance” and “intrusive surveillance”. The Council can only authorise directed surveillance (as defined later in this document) and **cannot** “bug” properties or individuals.

Covert Human Intelligence Source (CHIS)

In a few investigations it is necessary and appropriate to use a human source that provides information in confidence and may also involve seeking information from a party who does not know that the information will be given to the investigator. The procedures set out in this document are intended to maintain safety, integrity and compliance with legislation by strictly controlling and regulating the relationship between the Council and a human intelligence source.

A Council officer who:

- establishes a relationship with another person to obtain information (without disclosing that purpose), or
- encourages a third party to establish or use a relationship with someone to obtain information, and to pass it on without that person’s knowledge

is acting as (or directing) a “covert human intelligence source” often referred to as undercover officers or the use of informants. Such activity may also breach an individual’s human rights and is therefore controlled by RIPA. The use of an “informant” that has been tasked to obtain information can be particularly involved and should only be used in special circumstances. The use of any human intelligence source must always be **formally authorised**.

Acquisition of Communications Data

The Council **cannot** obtain the content of phone calls, e-mails or postal communication. They can obtain the subscriber and billing details and where necessary the called and received numbers. Such activity would also breach an individual’s human rights and is therefore strictly controlled and is required to be **formally authorised**. The authorisation process must comply with an approved Code of Practice and be carried out by specialist trained Officers. Consideration must also be given to the requirements of the Data Protection Act in respect of the subsequent retention, use and storage of data or information obtained.

In cases of conflict between the Policy or Reference Guide and relevant statutes or the statutory Code of Practice, the statute or statutory Code shall prevail.

Surrey County Council Policy on the use of Surveillance and the Acquisition of Communication Data

In carrying out investigations into the alleged illegal activities of individuals and organisations, the Council will seek to ensure that any interference with the rights of any person is lawful, necessary and proportionate to the objectives of the investigation. In particular, the Council recognises that any use of covert surveillance by its staff (and others acting on its behalf) should be in accordance with the requirements of the Regulation of Investigatory Powers Act 2000 (as amended) and any statutory Code of Practice. Also, that the acquisition of communications data will be in accordance with the requirements of that Act and in addition the Regulation of Investigatory Powers (Communications Data) Order 2000 (as amended) and the statutory Codes of Practice.

To ensure compliance with the above, the Council has formally adopted and published this policy and guidance for officers.

Service Managers are required to ensure that officers and services act in compliance with this policy and guidance.

1 Reference Guide to procedures

- 1.1 This Reference Guide sets out the Council's procedures for the authorisation and conduct of covert surveillance operations, covert human intelligence sources and the obtaining of communications data. It provides a brief summary of the main requirements of relevant law and the Statutory Code of Practice.
- 1.2 The Guide is an aide for clarification and is not a substitute for the legislation or the Code itself, which must be regarded as the definitive reference material.
- 1.3 The Trading Standards service takes the lead for the County Council in relation to RIPA and the central file of authorisations is retained by the Head of Trading Standards who has the role of corporate RIPA Monitoring Officer.
- 1.4 All authorisations, reviews, renewals and cancellations, in their original form, must be submitted to the RIPA Monitoring Officer as soon as possible after they are granted, and a copy retained by the submitting service. The RIPA Monitoring Officer will retain all such documentation in a RIPA file. The RIPA Monitoring Officer is responsible for central quality control of all RIPA authorisations and documentation and should review each on receipt. He should ensure that all reviews and cancellations are carried out within any time limits set. The RIPA Monitoring Officer is responsible for ensuring that all authorising officers are adequately trained and that there is an effective policy for the heightening of RIPA awareness throughout the Council.

- 1.5 Where services other than Trading Standards wish to seek authorisation for activities covered by RIPA they should seek guidance from Legal Services or from the Trading Standards Service
- 1.6 The Council scheme of delegation identifies those posts which are able to authorise directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). Those posts are highlighted in paragraph 4.2. No other officers may authorise these activities.

2 What is “surveillance”?

- 2.1 Surveillance includes monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications. (NB surveillance does not necessarily involve the use of devices like binoculars, tape recorders or cameras.)
- 2.2 RIPA applies controls on “**directed surveillance**” and “**intrusive surveillance**”. **The Council can only authorise directed surveillance.**
- 2.3 Special restrictions apply to the interception of any communications (See section 3.7 and 12)

3. What is “Directed Surveillance”?

- 3.1 Surveillance will be “directed surveillance” if it is:
 - covert (i.e. intended to be carried out without the person knowing); and
 - undertaken for a specific operation (as opposed to, for example, routine CCTV surveillance of an area); and
 - carried out in such a way as to make it likely that private information will be obtained about any person (NB: not necessarily the person ‘targeted’).
- 3.2 “Private information” includes any information relating to a person’s private or family life. This phrase should be interpreted widely, and considered to include all manner of personal information including personal telephone calls made from work and business matters which are not intended to be public.
- 3.3 Secretly recording anything overtly observed or heard will be considered covert surveillance, e.g. secretly recording a phone call you make or receive.
- 3.4 Surveillance will not be covert (and will therefore be outside the definition of “directed surveillance” and not require RIPA authorisation) if the subject has been warned of it. Surveillance by CCTV (fixed or mobile) will not be covert if there is adequate signage.
- 3.5 Surveillance carried out in or into residential premises or any private vehicle, where the observer is present in the premises or vehicle or uses a surveillance device giving an equivalent quality of information is called

“intrusive surveillance” and local authorities cannot authorise such surveillance.

3.6 Special rules apply to the interception of communications. The Council is not permitted to intercept private mail or communications. Nor are they allowed to secretly monitor phone calls, emails, etc during the course of transmission (or to record them during transmission for possible subsequent monitoring) unless:

- either, the sender or recipient has consented,
- or the monitoring is of a Surrey County Council system for a purpose such as to detect unauthorised use. In the latter case, RIPA authorisation may not be required, as a general authorisation for ‘internal’ monitoring is contained in The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. However, strict conditions apply and anyone considering such monitoring should read the Regulations and take appropriate legal advice before proceeding. In particular, potential users of the system must have been made aware that monitoring might take place and hence the need for a published email policy allowing for the monitoring of emails sent from or received at work. It is also worthy of note that DPA guidance suggests that RIPA-type considerations should still be applied and an "Impact Assessment" made. (See the DPA Code of Practice)

3.7 All applications, authorisations, reviews and renewals require a consideration of proportionality and necessity. In considering these concepts regard should be made to each of the following:

Necessity: Whether the proposed covert surveillance is necessary for the purposes of preventing or detecting crime or preventing disorder and why it is necessary to use covert surveillance in the operation under consideration.

Proportionality: Is the proposed covert surveillance proportional to the mischief being investigated; b. Is the proposed covert surveillance proportional to the anticipated intrusion on the target and others. c. Have other overt means of acquiring the evidence been considered and discounted..

4 The authorisation process for surveillance under RIPA

4.1 Directed surveillance may only be undertaken with proper authorisation, which will ensure that the principles of **legality, necessity and proportionality** are properly considered.

Before surveillance may be carried out, the Investigating Officer must:

- complete an application form seeking authorisation
- obtain signed authorisation on that form from a designated authorising officer.

4.2 The County Council authorises the following designated officers to authorise surveillance. These Officers hold a role or rank as specified in the

Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.

Head of Trading Standards
Assistant County Trading Standards Officer
Trading Standards Investigations Team Manager
Head of Legal Services

Where an authorisation may involve a “vulnerable” or juvenile source, RIPA requires that the authorization must come from the Chief Executive or in his / her absence a Strategic Director. The local authority has not in the past made any such authorization and it is extremely unlikely to need to do so in the future. In any such event legal advice must be obtained with reference to the legislation and Codes of Practice.

- 4.3 In all cases, authorising officers must be suitably trained and competent

5 Surveillance that might involve collateral intrusion

- 5.1 Collateral intrusion is where a third party’s privacy is infringed (e.g. where in monitoring the target individual an officer also observes, records or photographs one or more innocent third parties, this could be considered “collateral intrusion”).
- 5.2 Where authorisation for surveillance is requested, the authorising officer will, amongst other things, have to be satisfied that the risks of collateral intrusion have been considered and minimised and that any intrusion into privacy that may still occur is proportionate to what is sought to be achieved by the surveillance.
- 5.3 Accordingly, investigating officers will need to consider the potential for collateral intrusion in identifying possible locations for surveillance.
- 5.4 If directed surveillance unexpectedly gives rise to intrusion into a third party's privacy, the investigating officer should bring this to the attention of the Authorising Officer, so that the continuation of the authority can be reviewed and the decision recorded. If the collateral intrusion renders the surveillance disproportionate, then the authority should be cancelled and a new application made, if appropriate.

6 Surveillance where it is likely that ‘confidential material’ will be obtained

- 6.1 Confidential information includes people's communications with their solicitor or minister of religion, journalistic material, medical records and other matters which have particular sensitivity or where one would expect a particularly high level of privacy.
- 6.2 If, exceptionally, an investigating officer thinks that confidential information may be obtained in the course of conducting surveillance, then authorisation must be obtained from the most senior officers, namely Chief Executive or (in

his absence) Strategic Director. The local authority has not needed to do this previously and is unlikely to do so in the future. However the Office of Surveillance Commissioners has asked that provision for this be included in any corporate policy.

- 6.3 In all cases, authorising officers must be suitably trained and competent.

7 Where there is genuine urgency

- 7.1 If surveillance is required to be undertaken urgently, oral authorisation may be given. Oral authorisation is for use where an investigating officer believes that an operation would be jeopardised if the surveillance were not undertaken but there is insufficient time to obtain written authorisation. (NB. this process is not available where the officer simply omits to seek authorisation early enough). The authorising officer must subsequently complete the Authorisation Form and indicate why the matter was deemed urgent. The officer receiving the authorisation should also record (preferably in an official notebook) the circumstances of the authorisation.
- 7.2 Authorisation is not necessary if an officer undertakes limited surveillance as an immediate response to an event he encounters, where it would be impracticable to seek authorisation.

8 Authorisations for Surveillance Time Limits

- 8.1 Written authorisation for directed surveillance is valid for three months, but must be reviewed by the authorising officer at least every month. The authorising officer should complete the Review Form after carrying out the review.
- 8.2 If it is necessary to continue the surveillance for longer than three months, an application for a renewal of authorisation for surveillance must be made on Renewal Form before the authorisation ceases to have effect. A renewal will have effect for three months immediately following the expiry of the authorisation..
- 8.3 Oral authorisation runs for 72 hours from the time given. If the surveillance is required to continue past that period then written authorisation for a renewal must be sought.

9 Cancellation of Authorisation of Surveillance

- 9.1 At the end of any surveillance that has been carried out, the authorising officer must complete Cancellation Form to cancel the authorisation for surveillance and in any event before the expiry of any authorisation or renewal.

10 Officers Keeping and Destroying Records of Surveillance

- 10.1 All investigating officers have a legal obligation under the Criminal Procedures and Investigations Act 1996 to keep full and accurate records of criminal investigations. This would include all RIPA documentation and the results of the surveillance undertaken. In many circumstances there are legal obligations to disclose anything relevant to an affected party, and we may also have to demonstrate fairness and propriety to a court or tribunal reviewing what we have done.
- 10.2 Copies of authorisations, renewals and cancellations given should be retained on the investigation file and investigating officers must record:
- an account of events observed and/or conversations overheard (preferably in an official notebook)
 - a full account of any surveillance which has taken place in or on a private place (permitted only in order to maintain contact with a moving target or to assess whether the target has been lost)
 - reasons for, and the nature of, any inadvertent intrusion in or into a private place, and the results
 - reasons for selecting a specific target if authorised only for general observations
 - all records shall be kept in a safe and secure manner
- 10.3 A record of authorisations granted (copies of all the forms involved) must be kept in a safe and secure manner. The Trading Standards Service retains the central file of all authorisations and a copy of every authorisation granted needs to be forwarded to Trading Standards together with copies of any associated, reviews, renewals and cancellations.
- 10.4 Ultimately, all material gathered by surveillance must be destroyed (treat as confidential waste). Where a case goes to court, the material should be retained until there is no longer any prospect of any appeal against the court's decision (or, if a sentence of imprisonment is ordered in a criminal case, until the defendant has served the sentence). Should no action ultimately be taken in any case, surveillance material should be destroyed forthwith. Data Protection Act requires that data is not kept longer than necessary.

11 Acquisition of Communications Data under RIPA

- 11.1 There are circumstances when communications data is permitted to be obtained from Communications Service Providers (CSPs). Communications data does not include the content of any communication, but is information about the circumstances in which a communication has been sent, this applies to postal, telephone and Internet services.
- 11.2 RIPA defines the three types of communications data that can be obtained from the CSPs: subscriber information e.g. names and addresses of people to whom services are provided; service use information e.g. itemised telephone billing records; and traffic data e.g. information identifying the location from which a communication has been made. The local authority can only seek subscriber data and service use information but **NOT** traffic

data. More practical guidance on the processes and procedure for making Communications data checks has been developed by the Trading Standards service and is available directly from Trading Standards.

- 11.3 The authorisation process must comply with the approved Code of Practice and includes completion of all the necessary Forms. The final decision and submission must be by a named senior Officer who has been trained, tested and specifically authorized by the Home Office. There are currently five Officers within the Trading Standards Service of Surrey County Council able to request this type of information. These Officers have unique Home Office issued numbers and hence no other Officers in the Council should be able to obtain this type of information from the CSPs.
- 11.4 The principles of record keeping and destruction should, where applicable be applied as shown above (Section 10).

12 Covert Human Intelligence Sources (CHIS)

- 12.1 The most common use of this technique will be the use of an officer who is required to develop a relationship with an individual without disclosing that they are doing so on behalf of the Council, for the purposes of an investigation, for example when attempting to carry out a test purchase. Particular care must be taken to consider the safety and welfare of the officer.
- 12.2 The other less frequent use would be of an “informant” or similar party who is then tasked or encouraged to try to obtain information from another party, without disclosing the intention. The information obtained is then relayed to the Council for the purposes of an investigation. Of particular concern in these types of events must be the safety and welfare of the people involved (officer and “informant”). Also there must be strict control about information regarding the identities of those involved. As this type of investigatory technique requires particular care and control it should only be considered for use in investigation when no other option is available. Legal advice should be sought prior to any such operation in conjunction with advice from specialist officers in Surrey Police.
NOTE: Each CHIS will require management by a handler and controller. Records must be kept by a record maker in accordance with the Code of Practice for CHIS and the RIPA(Source Records) Regulations SI 2000/2725.
- 12.3 The authorisation process must comply with the approved Code of Practice and includes completion of all the necessary Forms. The principles outlined in Section 4, 5, 6, 7, all apply. The County Council has designated the specific officers/postholder under the corporate Scheme of Delegation to authorise the use of Covert Human Intelligence Sources. These Officers hold a role or rank as specified in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.
- 12.4 The list of postholders is found at paragraph 4.2
- 12.5 The Time Limits for the authorisation of Covert Human Intelligence Source shall be no more than 12 months and 72 hours for urgent oral authorisations.

Reviews should take place as appropriate and as frequently as considered necessary and practical by the authorising officer.

- 12.6 The principles outlined in Section 9 apply but in addition where necessary, the safety and welfare of the source should continued to be taken into account.
- 12.7 The principles of Section 10 apply however particular care must be exercised for the safe and secure storage and eventual destruction of any record.

13 Training

- 13.1 Any Unit/Service that proposes to undertake directed surveillance, covert human intelligence sources, or obtaining permitted communications data, must first ensure that all relevant staff have received sufficient instruction to enable them to comply with RIPA and the various Codes of Practice. They will then need to be added to the Authorised Officer List, and in the case of obtaining communications data have undergone Home Office recognised and accredited training.

14 Management Monitoring and Annual Report

- 14.1 Any service that undertakes directed surveillance, the use of covert human intelligence sources and acquisition of communications data should have in place a system of auditing to ensure that staff involved have had the necessary instruction to comply with RIPA and the Codes of Practice and that all the requisite procedures are consistently followed.
- 14.2 The procedures and records referred to in this Protocol are subject to inspection by Office of the Surveillance Commissioner (in relation to Surveillance and Covert Human Intelligence Sources) and the Interception of Communications Commissioner's Office (in relation to communication data).
- 14.3 The RIPA Monitoring Officer for the County Council is the Head of Trading Standards who maintains the central record of RIPA authorisations.
- 14.4 The Trading Standards Manager / Head of Trading Standards will produce an annual review of all corporate RIPA activity each year, which will summarise the range of issues for which RIPA authorisation was granted. The report will be submitted to the Head of Legal Services and to the Safer and Stronger Communities Select Committee. The review will include a summary of the results of any external inspection by the Office of Surveillance Commissioners and the Interception of Communications Commissioners Office. The report will then be published, with a view to ensuring openness, transparency and enhancing public confidence in the application of RIPA by the local authority.

15. Forms

- 15.1 Copies of all current RIPA forms for Directed Surveillance, Covert Human Intelligence Sources, Communications checks are retained by and are available from the Trading Standards Service.

16. Contact Officers

- 16.1 Various officers can be contacted for further information and advice on the application of RIPA

Peter Denard	Head of Trading Standards
Steve Ruddy	Assistant County Trading Standards Officer
Katherine Preston	Trading Standards Investigations Team Manager

- 16.2 For Communications Data Checks the trained and Home Office accredited officers (SPOCs) are:

Katherine Preston
Steve Playle
Michele Manson
Keith Vivers
Tanya Griffiths