

SURREY COUNTY COUNCIL

POLICY & PROTOCOL

ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000

&

THE PROTECTION OF FREEDOMS ACT 2012

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

Scope

This Protocol applies to Directed Surveillance, Covert Human Intelligence Sources and the Acquisition of Communications Data 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 local authorities for the **prevention of disorder or the prevention/detection of crime**.

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.

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

The Protection of Freedoms Act 2012 has introduced two significant changes to the use of RIPA

1) All local authority authorisations to use RIPA can only be given effect once an order approving the authorisation is given by a Justice of the Peace.

2) Applications for directed surveillance by local authorities must first meet the 'directed surveillance crime threshold'. Directed surveillance may only be authorised to prevent or detect criminal offences that;

- Are punishable by a maximum term of at least 6 months imprisonment, or,
- Are related to the sale of alcohol or tobacco to underage persons.

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.

Directed Surveillance

Directed 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 directed 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 and Criminal Procedure and Investigations Act 1996 in respect of the subsequent retention, use and storage of data or information obtained.

Where directed 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 directed 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.

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/she 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 must 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, the use of Covert Human Intelligence Sources (CHIS) and applications for Communications Data. 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.
(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.**

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’).
 - Targeted use of electronic surveillance. Such as;
 - ANPR (Automatic Number Plate Recognition), which can be used in conjunction with CCTV systems to track the movements of a vehicle by reference to the number plate.
 - Social Media, which can be used to interact with, record or monitor information about a person.
- 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 made 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 and it is not used to target an individual.
- 3.5 Surveillance carried out in or into residential premises or any private vehicle, 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

covertly monitor phone calls, emails, etc during the course of transmission (or to covertly record them during transmission for possible subsequent monitoring). Unless it is doing so under the separate provisions of the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

- 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:

- A. 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 Directed 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.

Applications for directed surveillance only must first meet the 'directed surveillance crime threshold'. Directed surveillance may only be authorised to prevent or detect criminal offences that;

- Are punishable by a maximum term of at least 6 months imprisonment, or,
- Are related to the sale of alcohol or tobacco to underage persons.

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.

Once this is complete the application and accompanying paperwork must be prepared and presented for **judicial approval** by a **Justice of the Peace (JP)**. The JP **must be satisfied** that on the papers submitted that the **application is legal, necessary and proportionate**. This presentation will be made in private by one of the Senior Legal Officers within the Trading Standards service, or a similarly experienced officer.

- 4.2 The County Council authorises the following designated senior 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 Head of Trading Standards

Where an authorisation may involve a “vulnerable” or juvenile source, RIPA requires that the authorisation 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 authorisation 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 and where appropriate operations must be risk assessed.

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.
- 5.5 In the unlikely event of collateral intrusion, it will be dealt with in accordance with statutory and internal policies and procedures.

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

- 6.1 Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material as defined within sections 98 to 100 of the Police Act 1997.
- 6.2 Confidential information includes people's communications with their solicitor or minister of religion, journalistic material, medical records, communications between a Member of Parliament and another on constituency matters, and

other matters which have particular sensitivity or where one would expect a particularly high level of privacy.

- 6.3 If, exceptionally, an investigating officer thinks that confidential information as detailed within paragraph 6.1 and 6.2 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/her 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.
- 6.4 In all cases, authorising officers must be suitably trained and competent.

7 Authorisations for Surveillance Time Limits

- 7.1 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.
- 7.2 If it is necessary to continue the surveillance for longer than three months, an application for the renewal of authorisation for surveillance must be made on a renewal form before the authorisation ceases to have effect. A renewal will have effect for three months immediately following the expiry of the previous authorisation. The process for renewing an authorisation is identical in all respects to that of an initial application.

8 Cancellation of Authorisation of Surveillance

- 8.1 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 do so before the expiry of any authorisation or subsequent renewal.

9 Officers Keeping and Destroying Records of Surveillance

- 9.1 All investigating officers have a legal obligation under the Criminal Procedure 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.
- 9.2 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
- 9.3 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.
- 9.4 Ultimately, all material gathered by surveillance must be destroyed in accordance with best practice and data retention policy (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.

10 Acquisition of Communications Data under RIPA

- 10.1 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.
- 10.2 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 or to 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 process and procedure for making Communications data checks is available directly from Trading Standards.
- 10.3 The authorisation process must comply with the approved Code of Practice and includes completion of all the necessary Forms. The principles outlined in Sections 4, 5, & 6 all apply. The County Council has designated specific officers/postholders under the corporate Scheme of Delegation to authorise the use of Communication data checks. Those posts are highlighted in paragraph 4.2. No other officers may authorise the acquisition of communications data.
- 10.4 Once this is complete the application and accompanying paperwork must be prepared and presented for **judicial approval** by a **Justice of the Peace (JP)**. The JP **must be satisfied** that on the papers submitted that

the **application is legal, necessary and proportionate**. This presentation will be made in private by one of the Senior Legal Officers within the Trading Standards service or a similarly experienced officer.

- 10.5 All requests of this type are submitted through a service provided by the National Anti Fraud Network (NAFN) who contact CSP's as a Single Point of Contact (SPoC) on our behalf and provide us with the results.
- 10.6 The SPoC is an officer who has undergone formal training with the Home Office, is independent from the investigation, will advise the applicant, and will submit applications for authorisation if, and only if, they meet all the formal requirements, including those of necessity and proportionality. Authorisation is then given by the Designated Senior Officer, also independent from the investigation. If the application is authorised, it is returned to the SPoC officer who will obtain the communications data from the CSP and pass it to the applicant. Officers able to act as designated officers and SPoC's are found at paragraph 15.
- 10.7 The principles of record keeping and destruction should, where applicable be applied as shown above (Section 9).

11 Covert Human Intelligence Sources (CHIS)

- 11.1 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 certain types of test purchase. Particular care must be taken to consider the safety and welfare of the officer.
- 11.2 The other less frequent use would be of an "informant" or similar party who obtains information from another party, without disclosing the intention and the information obtained is then relayed to and used by 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") and risk assessments must be carried out and recorded. 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 in exceptional circumstances. Legal advice should be sought prior to any such operation in conjunction with advice from specialist officers in Surrey Police.

In such exceptional circumstances a 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.

- 11.3 The authorisation process must comply with the approved Code of Practice and includes completion of all the necessary Forms. The principles outlined in Sections 4, 5, & 6, all apply. The County Council has designated specific officers/postholders under the corporate Scheme of Delegation to authorise

the use of Covert Human Intelligence Sources. Those posts are highlighted in paragraph 4.2. No other officers may authorise these activities.

- 11.4 Once this is complete the application and accompanying paperwork must be prepared and presented for **judicial approval** by a **Justice of the Peace (JP)**. The JP **must be satisfied** that on the papers submitted that the **application is legal, necessary and proportionate**. This presentation will be made in private by one of the Senior Legal Officers within the Trading Standards service, or a similarly experienced officer.
- 11.5 The Time Limits for the authorisation of Covert Human Intelligence Source shall be no more than 12 months. Reviews should take place as appropriate and as frequently as considered necessary and practical by the authorising officer.
- 11.6 The principles outlined in Section 8 apply but in addition where necessary, the safety and welfare of the source should continue to be taken into account.
- 11.7 The principles of Section 9 apply however particular care must be exercised for the safe and secure storage and eventual destruction of any record.

12 Surveillance of Social Media/Online Selling Platforms

- 12.1 Over the last decade the way the world communicates has changed and continues to do so as new technology and applications are developed .As such, public authorities should be able to use the internet in a safe and responsible way to protect the people it serves.
- 12.2 When considering surveillance of social media or online selling platforms there is an expectation of privacy. The RIPA codes of practice are clear in the definition of private and family life as prescribed in ARTICLE 8 Human Rights Act. These should be considered broadly.
- 12.3 *Right to respect for private and family life*

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Any such interference would need RIPA consideration

- 12.5 Authorising Officers should not assume that one service provider is the same as another or that services provided by a single provider are the same. Whilst it is an individual's responsibility to set privacy settings to protect private information, and even though data may be deemed to be published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available. The author will have a reasonable expectation of privacy if access controls are applied.

- 12.6 Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. **However, repeat viewings of 'open source' sites may constitute directed surveillance on a case by case basis and this should be borne in mind.**
- 12.7 If it is necessary and proportionate for a public authority to covertly breach access controls, the minimum requirement will be an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than merely reading the site's content.)
- 12.8 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.
- 12.9 For officers where RIPA authorisation has been deemed not required, there needs to be clear direction around what can and cannot be done:
1. No setting up of false profiles
 2. No bypassing security settings
 3. No gathering of private information
 4. No repeated viewing of individuals accounts even when public and unprotected
- 12.10 Any research should be recorded containing the date and sites visited and the reason. Records should be made available for inspection by the Investigatory Powers Commissioner's Office.
- 12.11 These control measures should eliminate the risk of basic online research becoming online surveillance.
- 12.12 If research identifies a need to capture online evidence of an offence by means of a screen shot then this should be recorded and stored in-line with local policy.

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 the Investigatory Powers Commissioner's Office.
- 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 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. The review will include a summary of the results of any external inspection by the Investigatory Powers Commissioner's Office. The annual 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 and Communications checks are retained by and are available from the Trading Standards Service.

13 Compliance with the General Data Protection Regulation 2018 and the Data Protection Act 2018

- 16.1 Surrey County Council are the Data Controller under these legal requirements and will determine the purpose and means of processing the personal data they hold. Trading Standards fulfils the role of the Data Processor as they bear responsibility for the processing of personal data. To comply with the General Data Protection Regulation there must be a lawful basis identified before the personal data can be processed. Further details can be found via the following link <https://www.surreycc.gov.uk/your-council/your-privacy>

17 Contact Officers

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

Jason Russell	Executive Director for Highways, Transport and Infrastructure (Senior Responsible Officer)
---------------	---

Steve Ruddy	Head of Trading Standards (Monitoring Officer)
-------------	---

Amanda Poole	Assistant Head of Trading Standards
--------------	-------------------------------------

17.2 Designated Senior officers who may authorise Communications Data Checks are:

Steve Ruddy Head of Trading Standards

Amanda Poole Assistant Head of Trading Standards