

Kent County Council

Policy in relation to the use of covert investigative techniques

Contents

Introduction	2
Policy Statement	3
Internet and Social Media investigations	4
Obtaining Authorisation	5
Duration of authorisations	5
Reviews	6
Renewals	6
Cancellations	6
Central Register and Monitoring	6
Training	7
Planned and Directed Use of Council CCTV Systems	7
Special Arrangements	7
Oversight	7
Use of Artificial Intelligence (AI)	8
Glossary	9
Annex 1 – Surveillance forms	10
Annex 2 – Covert Human Intelligence forms	11
Annex 4 – Guidance on completing surveillance forms	12
Annex 5 – Guidance on completing Covert Human Intelligence forms	14

1. Introduction

This policy document is based on the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) as amended, The Protection of Freedoms Act 2012, The Investigatory Powers Act 2016 and the Home Office's Codes of Practice for Directed Surveillance, Covert Human Intelligence Sources (CHIS) and Acquisition and Disclosure of Communications data.

Links to the above documents can be found at:

<http://www.legislation.gov.uk/ukpga/2000/23/contents>

<http://www.legislation.gov.uk/ukpga/2012/9/contents>

<http://www.legislation.gov.uk/ukpga/2016/25/contents>

<https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice/covert-surveillance-and-property-interference-code-of-practice-accessible>

https://assets.publishing.service.gov.uk/media/63985c2fe90e077c2e1ce84c/Revised_CHIS_Code_of_Practice_December_2022_FINAL.pdf

https://assets.publishing.service.gov.uk/media/68419a3d58bd5a53d0211cf7/Communications_Data_Code_of_Practice_-_June_2025.pdf

- 1.1 Surveillance plays a necessary part in modern life and law enforcement. It is used not just in the targeting of criminals, but also as a means of preventing crime and disorder. The Regulation of Investigatory Powers Act 2000 (RIPA) introduced a system of authorisation and monitoring of activities, to ensure that the rights of the individual were not unnecessarily compromised in the pursuance of regulatory compliance. The Protection of Freedoms Act and Investigatory Powers Act have refined the system introduced by RIPA.
- 1.2 Within the County Council, Trading Standards Officers may need to covertly observe and then visit a shop, business premises, website, social media page or to follow a vehicle or individual as part of their enforcement functions. During a visit or a test purchase situation it may be necessary to covertly video record a transaction, as it takes place. Environmental crime enforcement staff may also need to observe or record at places where illegal tipping or other similar crimes take place and access communications data when investigating such crimes. Similarly, KCC's Internal Audit fraud investigators may need to carry out covert surveillance or acquire communications data when they are investigating a crime which they intend to prosecute using the criminal law. They need to use covert surveillance techniques as part of their official duties.
- 1.3 Only those officers designated as "authorising officers" from the specified units or services are permitted to authorise the use of techniques referred to in RIPA. Trading Standards may use Covert Directed Surveillance, Covert Human Intelligence Sources and acquisition of communications data. Environmental

Crime enforcement team may use Covert Directed Surveillance and acquisition of communications data. Internal Audit fraud investigators may use Covert Directed Surveillance and acquisition of communications data.

- 1.4 Covert Directed Surveillance is undertaken in relation to a specific investigation or operation, where the person or persons subject to the surveillance are unaware that it is, or may be, taking place. The activity is also likely to result in obtaining private information about a person, whether or not it is specifically for the purpose of the investigation.
- 1.5 Investigations may also require the use of Covert Human Intelligence Sources (CHIS). These may be under-cover officers, agents or informants. Such sources may be used by the County Council to obtain and pass on information about another person, without their knowledge, as a result of establishing or making use of an existing relationship. This clearly has implications as regards the invasion of a person's privacy and is an activity which the legislation regulates. A CHIS (other than our own staff) would be used only rarely and in exceptional circumstances.
- 1.6 The Investigatory Powers Act (IPA) also requires a control and authorisation procedure to be in place in respect to the acquisition of telecommunications data. The County Council needs to comply with these requirements when obtaining, for example, telephone or internet subscriber, billing and account information.
- 1.7 In addition, the IPA put in place the Investigatory Powers Commissioner whose duties include inspection those public bodies undertaking covert surveillance and the acquisition of communications data and introduced an Investigatory Powers tribunal to examine complaints that human rights may have been infringed.

2. Policy Statement

- 2.1 Kent County Council will not undertake any activity defined within RIPA or the IPA without prior authorisation in the legally prescribed form.
- 2.2 The Corporate Director of Growth, Environment and Transport has been appointed as the overall Senior Responsible Officer (SRO) with responsibility for the use of covert techniques and, as such, has been given authority to appoint Authorising Officers for the purposes of RIPA (for surveillance and CHIS activities), a Senior Responsible Officer and "Made Aware" Officers for the purposes of the IPA (for access to communications data). The Corporate Director is a member of the corporate leadership team currently called Corporate Management Team.
- 2.3 The Authorising Officer will not authorise the use of surveillance techniques or CHIS unless the authorisation can be shown to be necessary for the purpose of preventing or detecting crime or of preventing disorder.
- 2.4 In addition, the Authorising Officer must believe that the surveillance or use of CHIS is lawful, necessary and proportionate to what it seeks to achieve. In making this judgment, the officer will consider whether the information can be obtained using other methods and whether efforts have been made to reduce the impact of the surveillance or intrusion on other people, who are not the subject of the operation.

- 2.5 Applications for authorisation of surveillance or the use of a CHIS will be made in writing on the appropriate form (see Annexes 1 or 2 for example forms).
- 2.6 Intrusive surveillance operations are defined as activities using covert surveillance techniques on residential premises or in any private vehicle, which involves the use of a surveillance device or an individual in such a vehicle or on such premises. Kent County Council officers are NOT legally entitled to authorise or undertake these types of operations. Operations must not be carried out where legal consultations take place at the places of business of legal advisors or similar places such as courts, police stations, prisons or other places of detention.
- 2.7 Public bodies are permitted to record telephone conversations, where one party consents to the recording being made and an appropriate authorisation has been granted. On occasions, officers do need to record telephone conversations, to secure evidence.
- 2.8 It is the policy of this authority to be open and transparent in the way that it works and delivers its services. To that end, a well-publicised KCC Complaints procedure is in place and information on how to make a complaint will be provided on request being made to the Corporate Director or Authorising Officer.

3. Internet and social media investigations

- 3.1 On-line communication has grown and developed significantly over recent years. The use of this type of communication in the commission of crime is a recognised aspect of routine investigations.
- 3.2 Observing an individual's lifestyle as shown in their social media pages or securing subscriber details for e-mail addresses is covered by the same considerations as off-line activity.
- 3.3 Staff using the internet for investigative purposes must not, under any circumstances, use their personal equipment or their personal social media or other accounts.
- 3.4 KCC will provide equipment not linked to its servers for this purpose and will maintain a number of "legends" (false on-line personalities) for use in investigations. A register of all such legends will be maintained by the Trading Standards Service.
- 3.5 Under no circumstances will a legend include personal details of any person known to be a real person, including their photograph, or a name known to be linked to the subject of the covert technique.
- 3.6 A log will be maintained by the Trading Standards Service of the use of each legend. The log will include details of the user, time, date and enforcement purpose for which the legend is used. The log will be updated each time a legend is used.

- 3.7 It is unlikely that single viewing of open source data will amount to obtaining private information and it is therefore unlikely that an authorisation will be required. If in doubt, the investigating officer should consult a RIPA Authorising Officer.
- 3.8 Where data has restricted access (e.g. where access is restricted to “friends” on a social networking site), an application for CHIS and, if appropriate, directed surveillance should be made before any attempt to circumvent those access controls is made.

4. Obtaining Authorisation

- 4.1 The Corporate Director will designate by name one or more Directors, Heads of Service, Service Managers or equivalent to fulfil the role of Authorising Officer (for the purposes of Surveillance and CHIS authorisation), Senior Responsible Officer and “Made Aware” Officers (for the purposes of access to communications data). The Corporate Director will cause to be maintained a register of the names of such officers.
- 4.2 Where a CHIS is a juvenile or a vulnerable person, or there is the likelihood that the information acquired by covert surveillance will be Confidential Information (see Glossary), then the authorisation must be from the Head of Paid Service or, in their absence, a Corporate Director nominated by the Head of Paid Service to deputise for them. In the event of such circumstances, the KCC General Counsel will also be informed.
- 4.3 Authorisations from the Authorising Officer for directed surveillance or to use a CHIS shall be obtained using the appropriate application form (see annexes 1 and 2 for example forms). Also see Section 12 in relation to CHIS.
- 4.4 Applications for access to communications data shall be made using the system provided by the National Anti-Fraud Network.
- 4.5 Guidance for completing and processing the application forms is attached (annexes 3 or 4). Guidance for use of the NAFN portal is published and updated on that website.
- 4.6 If authorisation is granted by the Authorising Officer, the applicant, or a suitably experienced officer nominated by the applicant, will make the necessary arrangements to secure judicial approval of the authorisation in compliance with the requirements of the Protection of Freedoms Act 2012. This requires the applicant, or their nominee, to attend a Magistrates’ Court and seek an approval order.

5. Duration of authorisations

- 5.1 All records shall be kept for at least 3 years.
- 5.2 A written authorisation (unless renewed) will cease to have effect at the end of the following periods from when it took effect:
- a) Directed Surveillance - 3 months
 - b) Conduct and use of CHIS - 12 months

6. Reviews

- 6.1 Regular review of authorisations shall be undertaken by the relevant Authorising Officer to assess the need for the surveillance or CHIS to continue. The results of the review shall be recorded on the central record of authorisations (see annexes 1 or 2 for review forms). Where surveillance or CHIS activity provides access to Confidential Information or involves collateral intrusion, particular attention shall be given to the review for the need for surveillance or activity in such circumstances.
- 6.2 In each case, the Authorising Officer shall determine how often a review is to take place, and this should be as frequently as is considered necessary and practicable.

7. Renewals

- 7.1 If, at any time, an authorisation ceases to have effect and the Authorising Officer considers it necessary for the authorisation to continue for the purposes for which it was given, they may renew it, in writing, for a further period of:
- three months – directed surveillance
 - twelve months – use of a CHIS
 - (see annexes 1 or 2 for examples of renewal forms)
- 7.2 A renewal takes effect at the time at which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once provided they continue to meet the criteria for authorisation.

8. Cancellations

- 8.1 The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the Directed Surveillance or the use or conduct of the CHIS no longer meets the criteria for which it was authorised (see annexes 1 or 2 for examples of cancellation forms). When the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.
- 8.2 As soon as the decision is taken that Directed Surveillance should be discontinued or the use or conduct of the CHIS no longer meets the criteria for which it was authorised, the instruction must be given to those involved to stop all surveillance of the subject or use of the CHIS. The authorisation does not 'expire' when the activity has been carried out or is deemed no longer necessary. It must be either cancelled or renewed. The date and time when such an instruction was given should be recorded in the central register of authorisations and the notification of cancellation where relevant.

9. Central Register and Oversight by Corporate Director

- 9.1 A copy of any authorisation, any renewal or cancellation (together with any supporting information relevant to such authorisation or cancellation) shall be forwarded to the Corporate Director or a person nominated by them within 5

working days of the date of the application, authorisation, notice, renewal or cancellation.

9.2 The Corporate Director shall:

- (a) ensure that a register of the documents referred to in paragraph 9.1 above is kept;
- (b) monitor the quality of the documents and information forwarded;
- (c) monitor the integrity of the process in place within the Council for the management of CHIS;
- (d) monitor compliance with Part II of RIPA and with the Codes;
- (e) oversee the reporting of errors to the relevant Oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- (f) engage with the IPC inspectors when they conduct their inspections, where applicable; and
- (g) where necessary, oversee the implementation of post-inspection action plans approved by the relevant Oversight Commissioner.

10. Training

10.1 The Authorising Officers shall be provided with training to ensure awareness of the legislative framework.

10.2 All officers seeking to apply for authorisations must complete the KCC online training before doing so.

11. Planned and Directed Use of KCC CCTV Systems

11.1 KCC's CCTV systems shall not be used for Directed Surveillance, without the Corporate Director or other senior legal officer confirming to the relevant operational staff that a valid authorisation is in place.

12. Special Arrangements

12.1 The use of a CHIS can present significant risk to the security and welfare of the person. Each authorisation will have a specific documented risk assessment and the CHIS (and all members of any support team) will be briefed on the details of that assessment. Kent County Council has a Memorandum of Understanding with Kent Police for circumstances where the CHIS is not an employee or other agent working for or on behalf of the authority. In other circumstances such as a member of public, "whistle-blower" or informant then Kent Police will handle the operation of the CHIS. Kent Police will ensure the compliance with the Regulations, codes of practice and all other risks such as the security and welfare of the CHIS (and associated persons). Any necessary and relevant information will be provided following best practise as to not risk identifying CHIS unless this is appropriate and approved by Kent Police. In such cases, Kent Police are responsible for all records and monitoring processes.

13. Oversight

- 13.1 The Corporate Director shall ensure that this policy is reviewed on an annual basis by presenting a report of activity to the Governance and Audit Committee (or similar Committee). There shall also be brief details of all activity under this policy provided to the Corporate Director and shared with the appropriate Cabinet Member at such intervals between the annual reports as the Corporate Director sees fit.
- 13.2 Every two years the KCC General Counsel will review the policy, and also contact the Corporate Directors responsible for all other units and services within Kent County Council to inform them of any changes or alterations. The communication will also seek to highlight the details of the restrictions imposed by RIPA, the IPA and Human Rights legislation. Should any unit or service (other than those permitted by this policy) consider that any actions it may have taken (or are considering taking) might infringe this policy, they must be raised with the KCC General Counsel as soon as practicable.

14. Use of Artificial Intelligence (AI)

- 14.1 In line with the Investigatory Powers Commissioner's Office (IPCO) guidance on the scope of interest in Artificial Intelligence, Kent County Council recognises the potential for AI technologies to support covert investigatory activities.
- 14.2 Where AI systems, defined as software capable of autonomous decision-making, adaptive learning, or large-scale data processing, are used in connection with covert investigatory powers, such use must be explicitly documented and subject to the same authorisation, oversight, and proportionality assessments as traditional methods.
- 14.3 AI may be used to assist with the review and analysis of evidence; however, investigators remain fully responsible for verifying the accuracy and relevance of any AI assisted outputs.
- 14.4 Decisions must not be based solely on AI generated insights. Instead, AI should be viewed as a tool to enhance investigative efficiency, not to replace human judgment.
- 14.5 Where AI is used to review data received from a RIPA or IPA request, this must be clearly recorded in the investigation records, and consideration should be given to referencing these methods in disclosure management documents. This ensures transparency, accountability, and compliance with both statutory oversight, disclosure and data protection obligations.

Glossary

"Confidential information" consists of matters subject to legal privilege, confidential personal information, or confidential journalistic material.

"Directed Surveillance" is defined in section 26 (2) of RIPA as surveillance which is covert, but not intrusive (i.e. takes place on residential premises or in any private vehicle), and undertaken:

- (a) for the purpose of specific investigation or specific operation;
- (b) in such a manner 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 RIPA to be sought for the carrying out of the surveillance.

"A person is a Covert Human Intelligence Source" if:

- he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything within paragraph (b) or (c);
- he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

"Communications data", in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data—

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—

(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,

(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or

(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or

(c) which—

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,

(ii) is about the architecture of a telecommunication system, and

(iii) is not about a specific person,

but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.

Annex 1 – Surveillance forms

Application for Authorisation to Carry Out Directed Surveillance

Review of Directed Surveillance Authorisation

Cancellation of a Directed Surveillance Authorisation

Application of Renewal of a Directed Surveillance Authorisation

(Forms available at <http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/>)

Annex 2 – Covert Human Intelligence forms

Application for Authorisation of the Use or Conduct of a Covert Human Intelligence Source

Review of a Covert Human Intelligence Source Authorisation

Cancellation of an Authorisation for the use of or Conduct of a Covert Human Intelligence Source

Application for renewal of a Covert Human Intelligence Source Authorisation

(Forms available at <http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/>)

Annex 3 - Guidance on completing surveillance forms

Details of Applicant

Details of requesting officer's work address and contact details should be entered.

Details of Application

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171

Fill in details of Authorising Officer (see paras 3.1 and 3.2 of Policy)

2. Purpose of the specific operation or investigation

Outline what the operation is about and what is hoped to be achieved by the investigation. Indicate whether other methods have already been used to obtain this information. Give sufficient details so that the Authorising Officer has enough information to give the Authority e.g. "Surveillance at Oakwood House and Mr. X".

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used

Give as much detail as possible of the action to be taken including which other officers may be employed in the surveillance and their roles. If appropriate append any investigation plan to the application and a map of the location at which the surveillance is to be carried out.

4. The identities, where known, of those to be subject of the directed surveillance

5. Explain the information that it is desired to obtain as a result of the directed surveillance

This information should only be obtained if it furthers the investigation or informs any future actions

6. Identify on which grounds the directed surveillance is necessary under section 28(3) of RIPA

The ONLY grounds for carrying out Directed Surveillance activity is for the purpose of preventing or detecting crime or of preventing disorder.

This can be used in the context of local authority prosecutions, or where an employee is suspected of committing a criminal offence e.g. fraud.

7. Explain why this directed surveillance is necessary on the grounds you have identified (code chapter 3)

Outline what other methods may have been attempted in an effort to obtain the information and why it is now necessary to use surveillance.

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable (code chapter 3) Describe precautions you will take to minimise collateral intrusion

Who else will be affected by the surveillance, what steps have been done to avoid this, and why it is unavoidable?

9. Explain why the directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code chapter 3]

If the Directed Surveillance is necessary, is it proportionate to what is sought to be achieved by carrying it out? This involves balancing the intrusiveness of the activity on the target and others who may be affected by it against the need for the activity in operational terms. Reasons should be given why what is sought justifies the potential intrusion on the individual's personal life and his privacy. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

10. Confidential information (Code chapter 4)

Will information of a confidential nature be obtained (i.e. communications subject to legal privilege, or communications involving confidential personal information and confidential journalistic material) if so the appropriate level of authorisation must be obtained (see para 3.2 of the Policy).

12. Authorising Officer's Statement

13. Authorising Officer's comments

Must be completed outlining why it is proportionate and why he/she is satisfied that it is necessary.

Annex 4 - Guidance on completing Covert Human Intelligence forms

Details of Application

1. Authority Required

Fill in details of Authorising Officer (see paras 4.1 and 4.2 of the Policy)

Where a vulnerable individual or juvenile source is to be used, the authorisation **MUST** be given by the Head of Paid Service or, in their absence, the Corporate Director deputising for them.

2. Describe the purpose of the specific operation or investigation

Sufficient details so that the Authorising Officer has enough information to give Authority. Outline what the operation is about and the other methods used already to obtain this information.

3. Describe in detail the purpose for which the source will be tasked or used

Give as much detail as possible as to what the use of the source is intended to achieve.

4. Describe in detail the proposed covert conduct of the source or how the source is to be used

Describe in detail the role of the source and the circumstances in which the source will be used

5. Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA

The **ONLY** grounds for carrying out Directed Surveillance activity is for the purpose of preventing or detecting crime or of preventing disorder

6. Explain why this conduct or use of the source is necessary on the grounds you have identified (Code chapter 3)

Outline what other methods may have been attempted in an effort to obtain the information and why it is now necessary to use surveillance for the investigation.

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable (Code chapter 3)

Who else will be affected, what steps have been done to avoid this, and why it is unavoidable?

8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source? (see Code chapter 3)

Ensure that other authorities such as the police or other council departments are not conducting a parallel investigation or other activity which might be disrupted.

9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code chapter 6)

A risk assessment will have to be carried out to establish the risks to that particular source, taking into account their strengths and weaknesses. The person who has day to day responsibility for the source and their security (the 'Handler') and the person responsible for general oversight of the use made of the source (the 'Controller') should be involved in the risk assessment.

10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means? [Code chapter 3]

If the use of a Covert Human Intelligence Source is necessary, is it proportionate to what is sought to be achieved by carrying it out? This involves balancing the intrusiveness of the activity on the target and others who may be affected by it against the need for the activity in operational terms. Reasons should be given why what is sought justifies the potential intrusion on the individual's personal life and his privacy. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

11. Confidential information (Code chapter 4). Indicate the likelihood of acquiring any confidential information

Will information of a confidential nature be obtained (i.e. communications subject to legal privilege, or communications involving confidential personal information and confidential journalistic material) if so the appropriate level of authorisation must be obtained (see para 3.2 of the Policy).

13. Authorising Officer's comments

Must be completed outlining why it is proportionate and why he/she is satisfied that it is necessary to use the source and that a proper risk assessment has been carried out.