Policy in relation to the ~~regulation~~ use of ~~Investigatory Powers Act 2000~~ Covert Investigative Techniques

Contents

Introduction ~~to Regulation of Investigatory Powers~~ 2
Policy Statement 3
Internet and social media investigations 5
Obtaining authorisation 5
Retention and Duration of authorisations ..... ~~5~~6
Reviews 7
Renewals 7
Cancellations ..... ~~6~~7
Central Register and Monitoring 7
Training ..... ~~7~~8
Planned and Directed Use of Council CCTV Systems 9
Special Arrangements 9
Obtaining Judicial Approval of Authorisations 9
Data Protection Act 2018 11
Glossary ..... ~~10~~12
Annex 1 – Direct Surveillance forms ..... ~~12~~14
Annex 2 – Covert Human Intelligence forms ..... ~~13~~ 15
Annex 3 – Access to communications data forms ..... ~~14~~16
Annex 4 – Guidance on completing direct surveillance forms ..... ~~15~~17
Annex 5 – Guidance on completing Covert Human Intelligence forms ..... ~~17~~19
Annex 6 – Guidance on accessing communications data forms ..... ~~19~~21
Annex 7 – Guidance on Management of Covert Human Intelligence Sources 23
Annex 8 – ESCC Internal Guidance concerning Applications for use of Covert Investigative Techniques 25

1. Introduction ~~to Regulation of Investigatory Powers~~

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 (IPA) and the Home Office codes, namely the:

- Codes of Practice for Covert Surveillance and Property Interference
- Codes of practice for the acquisition, disclosure and retention of communications data, and;
- Covert surveillance and covert human intelligence sources codes of practice

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/collections/ripa-codes

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf

1.1 Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals, but also as a means of preventing crime and disorder. 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 Protections of Freedoms Act and IPA have refined the system introduced by RIPA.

1.2 Within the County Council, trading standards officers may for example need to covertly observe and then visit a shop or business premises as part of their enforcement function to verify the supply of goods or services. During this visit it may be necessary to covertly video record a transaction as it takes place.

1.3 Similarly, planning enforcement staff may need to observe the activities of companies involved in mineral extraction, to ensure that statutory requirements are being met. Officers from ~~Adult's~~ Adult and ~~Children's~~ Children Social Care,

Transport and Environment~~, Trading Standards~~ and other services may also all, on occasions, need to use covert surveillance techniques as part of their official duties when seeking to prevent or detect crime.

1.4 Covert Directed Surveillance is that 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 Our investigations may also require the use of Covert Human Intelligence Sources (CHIS). These may be undercover 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 who was not an officer of the County Council would be used only rarely and in exceptional circumstances.

1.6 The RIPA introduced a system of authorisation and monitoring of surveillance activities, to ensure that the rights of the individual were not unnecessarily compromised, in the pursuance of regulatory compliance. The ~~RIPA~~ IPA also requires a similar control and authorisation procedure to be in place in respect to the acquisition of communications data. The County Council will need to comply with these requirements when obtaining telephone subscriber, billing and account information and other communications data.

1.7 The Investigatory Powers Tribunal was introduced by the RIPA to examine complaints that human rights have been infringed. In addition, the ~~Investigatory Powers Act 2016~~ IPA put in place the Investigatory Powers ~~Commissioner's Office~~ Commissioner whose duties ~~are to keep under review the use~~ include inspection of ~~investigatory powers by~~ those public ~~authorities~~ bodies undertaking covert surveillance and the acquisition of communications data.

2. Policy Statement

2.1 East Sussex County Council will not undertake any activity defined within the RIPA or the IPA without prior authorisation from a trained, senior officer who is empowered to grant such consents. The Assistant Chief Executive has been appointed the Senior Responsible Officer for the purposes of RIPA and IPA and, as such, has been given authority to appoint Authorising Officers ~~(~~ for the purposes of surveillance ~~and CHIS~~ activities~~), Designated Persons and Single Points of Contact (~~ and "Made Aware" Officers (see Paragraph 8.5 of the Communications Data Code of Practice) for the purposes of access to communications data~~) under the Act.~~

2.2 The Authorising Officer ~~or Designated Person~~ will not authorise the use of surveillance techniques, covert human intelligence sources ~~or access to communications data~~ unless the authorisation can be shown to be necessary for the purpose of preventing or detecting crime or of preventing disorder.

2.3 In addition, the Authorising Officer ~~or Designated Person~~ must believe that the surveillance ~~and/or the obtaining of communications data~~ or CHIS is lawful, necessary and proportionate to what it seeks to achieve. In making this judgement, 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 on other people, who are not the subject of the operation.

2.4 The responsibilities set out in paragraph 9.2 of this policy shall be the specific responsibility of the Senior Responsible Officer. A ~~RIPA~~ Co-ordinating Officer designated by the Senior Responsible Officer will support the Senior Responsible Officer in the exercise of these responsibilities.

2.5 Applications for authorisation of surveillance, the use of a CHIS or the obtaining of communications data will be made in writing on the appropriate form (See annexes 1, 2 or 3).

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. East Sussex County Council officers are **NOT** legally entitled to authorise 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 However public bodies are permitted to record telephone conversations, where one party consents to the recording being made and ~~a Directed Surveillance~~ an appropriate authorisation has been granted. On occasions, officers of the County Council 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 Corporate Complaints procedure is in place and information on how to make a complaint to the Investigatory Powers Tribunal will be provided on receipt of a request by the Senior Responsible Officer.

2.9 **Elected members have the following responsibilities in connection with this policy and the County Council's use of the RIPA; they**

- should review the authority's use of RIPA and the IPA;
- should set the policy at least once a year;
- should consider internal reports on the use of RIPA and the IPA on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose; and
- should not be involved in making decisions on specific authorisations.

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 East Sussex County Council will provide equipment not linked to its servers for this purpose and will develop a number of "legends" (false on-line personalities) for use in investigations if necessary. 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 Although the viewing of open source data is unlikely to amount to obtaining private information and it is therefore unlikely that an authorisation will be required, repetitive viewing of open source sites for the purpose of intelligence gathering and data collation may require authorisation. If in doubt, the investigating officer should consult an 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~~ may be appropriate if, for example, a meaningful relationship is established or repeat monitoring of online activity is required.

4. Obtaining Authorisation

4.1 The Senior Responsible Officer shall 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) and ~~Designated Person and Single Point of Contact~~ "Made Aware" Officer (for the purposes of access to communications data). The Senior Responsible Officer shall maintain a register of the names of such officers.

4.2 Where the CHIS is a juvenile or a vulnerable person, or there is the likelihood that the information acquired will be Confidential Information then the authorisation must be from the Chief Executive or, in her absence, the Chief Operating Officer.

4.3 Authorisations from the Authorising Officer for directed surveillance or the use of a CHIS shall be obtained using the appropriate application form (see annexes 1 and 2).

4.4 Applications for access to communications data shall be made via the National Anti Fraud Network (NAFN) (see annexes 3 and 6) who will then arrange for it to be submitted to the Office for Communications Data Authorisations.

4.5 Guidance for completing the application forms is attached (annexes 4,5,or 6). Guidance for use of the NAFN portal is published and updated on the NAFN website.

4.6 Guidance on the management of CHIS is attached (annex 7).

4.7 Guidance on processing the applications is attached (annex 8).

5. Retention and Duration of authorisations

5.1 All records shall be kept for 5 years.

5.2 Unless renewed or cancelled, authorisations are valid, commencing at the date of judicial approval, for a period of:

- ~~a period of~~ 3 months (for directed surveillance) and
- 12 months for a CHIS (~~one month~~ four months if the person is a juvenile)

~~And not for lesser periods.~~

5.3 ~~A notice or~~ Unless renewed or cancelled an authorisation issued for the production of communication data will remain valid for one month commencing at the date ~~of judicial approval~~ upon which it is granted. A notice given under an authorisation remains in force until compiled with or until the authorisation under which it was given is cancelled.

6. Reviews

6.1 Regular review of authorisations and notices shall be undertaken by the relevant Authorising Officer to assess the need for the surveillance, authorisation or notice to continue (see annex 8 for guidance on the process). The results of the review shall be recorded on the central record of authorisations (see annexes 1 or 2 for review of directed surveillance or use of a CHIS forms). Where surveillance provides access to Confidential Information or involves collateral intrusion, particular attention shall be given to the review for the need for surveillance 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, the Authorising Officer considers it necessary for the authorisation or notice to continue for the purposes for which it was given, he or she may renew it, in writing, for a further period of:-

- three months – directed surveillance
- twelve months – use of a CHIS (four months if the person is a juvenile) ~~One month – access to communications data~~

(see annexes 1 or 2 for renewal forms of directed surveillance or use of a CHIS. Renewal of an authorisation or notice to obtain communications data is by means of a further authorisation or notice. See annex 8 for guidance on the process)

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. Authorisation 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 or notice must cancel it if he/she is satisfied that the Directed Surveillance, the use or conduct of the Covert Human Intelligence Source ~~or access to communcations data,~~ no longer meets the criteria for which it was authorised (see annexes 1 or 2 for cancellation of directed surveillance or use of a CHIS forms and annex 8 for guidance on the process). ~~Cancellation of an authorization or notice to obtain communcations data should be made in writing to the communication service provider.~~ 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. In respect of an authorisation or notice to obtain communications data, if the applicant becomes aware that the authorisation is no longer necessary or proportionate he/she should notify NAFN who must cease the authorised conduct. When it is appropriate to do so, a communications service provider should be advised of the cancellation of an authorisation, for example

where details of an authorisation have been disclosed to a communications service provider.

8.2 As soon as the decision is taken that Directed Surveillance should be discontinued or the use or conduct of the Covert Human Intelligence Source, 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 Senior Responsible Officer

9.1 A copy of any application, authorisation, notice, renewal or cancellation (together with any supporting information) shall be forwarded to the Senior Responsible Officer or a person nominated by them within 5 working days of the date of the application, authorisation, notice, renewal or cancellation.

9.2 The Senior Responsible Officer shall be responsible for:

(a) keeping a register of the documents referred to in paragraph 9.1 above;

(b) monitoring the quality of the documents and information forwarded to him;

(c) the integrity of the process in place within the public authority for the management of CHIS;

(d) monitoring compliance with Part II of the RIPA, Part III of the IPA and with the Codes;

(e) oversight of 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) engagement with the ~~IPCO~~ IPC inspectors when they conduct their inspections, where applicable;

(g) where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner;

(h) maintaining a RIPA/IPA training programme; and

(i) raising awareness of RIPA, the IPA and the ~~RIPA policy across the County Council~~ Policy in relation to the use of Covert Investigative Techniques.

10. Training

10.1 The Authorising Officers ~~Designated Persons and Single Points of Contact~~ shall be provided with training to ensure awareness of the legislative framework. ~~Single Points og Contact can only be appointed following attendance at a training course accredited by the Home Office and passing a written examination.~~

11. Planned and Directed Use of Council CCTV Systems

11.1 The Council's CCTV surveillance systems shall not be used for Directed Surveillance, without the Senior Responsible Officer or other senior legal officer confirming to the relevant operational staff that a valid authorisation is in place.

11.2 Also, regard must be had to the provisions of the Protection of Freedoms Act 2012, which required a regulatory framework for surveillance camera systems comprising a code of practice and a surveillance camera commissioner - see the Protection of Freedoms Act 2012 (Code of Practice for Surveillance Camera Systems and Specification of Relevant Authorities) Order 2013.

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 the assessment. The process is outlined in Annex 7. However, East Sussex County Council may use Sussex 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 Sussex Police may also be asked to handle the operation of the CHIS. In such cases Sussex Police would be required to ensure compliance with the RIPA, 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 by Sussex Police to East Sussex County Council, following best practice so as to not risk identifying CHIS unless this is appropriate and approved by Sussex Police. In such cases, Sussex Police would be required to be responsible for all records and monitoring processes.

~~12~~ 13. Obtaining Judicial Approval of Authorisations

~~12~~13.1 ~~Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval.~~ The Protection of Freedoms Act 2012 amended RIPA, to require that where an ~~a~~ Authorising Officer has granted an authorisation for the use of directed surveillance~~, acquisition of communcations data~~ or for the use of a CHIS, judicial approval will be required.

Authorising Officers must, when making authorisations, be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. The Council will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if at the date of the grant of authorisation or renewal of an existing authorisation if and only if, they are satisfied that:

a. there were reasonable grounds for believing that the use of the directed surveillance~~, acquisition of communications data~~ or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain.

b. the "relevant conditions" were satisfied in relation to the authorisation. Relevant conditions are that:

(i) the relevant person was designated as an Authorising Officer ~~or Designated Person~~;

(ii) it was reasonable and proportionate to believe that using covert surveillance~~, acquisition of communications data~~ or use of a covert human intelligence source was necessary and that the relevant conditions have been complied with;

(iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA; and

(iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

~~12~~ 13.2 Judicial approval will also review that the serious crime threshold has been met in relation to the carrying out of directed surveillance. This threshold is that the directed surveillance is for the purpose of preventing or detecting a criminal offence and meets the following conditions:

a. **that the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment; or**

b. **constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old) or**

c. constitutes an offence under section 92 Children and Families Act 2014 (sale of nicotine inhaling products to children under 18 years old) or proxy purchasing of tobacco, including nicotine inhaling products, to children under 18 years old under section 91 Children and Families Act 2014.

It is therefore essential that Investigating officers consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance

If the Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

~~12~~13.3 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates' Court to that authorisation has been obtained (see annex 8).

To ensure compliance with this requirement, any Authorising Officer who proposes to approve an application for the use of directed surveillance~~,~~ ~~acquisition of communications data~~ or for the use of a CHIS must immediately inform the RIPA Monitoring Officer by telephone or e-mail of the

details of the authorisation. The RIPA Monitoring Officer will then make the necessary arrangements for an application for an order to approve the authorisation to be made to the Magistrates' Court. The Authorising Officer and the Investigating Officer may be required to attend the Magistrates' Court to support the application.

~~13~~14. Data Protection Act ~~1998~~ 2018

~~13~~14.1 All data will be kept in accordance with the Data Protection principles and the Council's Information Governance policies.

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.

(See section 26 (8) of RIPA)

"Communications Data" as defined in section 261 (5) of IPA, is :-
~~(a) any traffic~~ 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 ~~or~~, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of ~~any potal service or~~ a telecommunication system by means of which ~~it~~ the communication is being or may be transmitted~~; (NOT AVAILABLE TO LOCAL AUTHORITIES)~~, or
~~(b) any information which includes none of the contents of a communication (apart from any information falling)~~

(iii)does not fall within sub-paragraph (~~a)) and is about the use made by any person(~~i) ~~of any postal~~ service or (ii) but does relate to the use of a telecommunications service~~;~~ or
~~(ii) in connection with the provision to or use by any person of any telecommunications services, of any part of~~ a telecommunication system~~;~~,

~~(c) any information not falling~~
(b)which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or
(c)which—
(i)is (or ~~(b) that~~ is is to be or is capable of being) held or obtained ~~in relation to persons to whom he provides the service, by~~ by, or on behalf of, a ~~person~~ providing telecommunications operator,
(ii)is about the architecture of a ~~postal service or telecommunications service~~ telecommunication system, and
~~(See section 21(4) RIPA)~~
(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 – Directed Surveillance forms

- Application for Authorisation to Carry Out Directed Surveillance
- Review of Directed Surveillance Authorisation
- Cancellation of a Directed Surveillance Authorisation
- Application for Renewal of a Directed Surveillance Authorisation

(Forms available at)
https://www.gov.uk/government/collections/ripa-forms--2

Authorising Officers are:

~~Liz Rugg, Assistant Director of Children and Families~~

~~Mark Stainton, Assistant Director Adult Social Care, Operations~~

Lucy Corrie, Head of Communities

Richard Strawson, Team Manager Trading Standards

~~Matthew Knowles~~ Paul Davison, Enforcement & Investigations Manager Trading Standards

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)

https://www.gov.uk/government/collections/ripa-forms-

Authorising Officers are:

~~Liz Rugg, Assistant Director of Children and Families~~

~~Mark Stainton, Assistant Director Adult Social Care, Operations~~

Lucy Corrie, Head of Communities

Richard Strawson, Team Manager Trading Standards

~~Matthew Knowles~~ Paul Davison, Enforcement & Investigations Manager Trading Standards

Annex 3 – Access to Communications Data forms

- Application for access to Communications Data

Applications must be made on the CycComms system which is available at www.nafn.gov.uk.

~~Designated Persons~~

Made aware officers are:

~~Lucy Corrie, Head of Communities~~

Richard Strawson, Team Manager Trading Standards

~~Matthew Knowles~~ Paul Davison, Enforcement and Investigations Manager, ~~Trading Standards~~

Annex 4 - Guidance on completing Directed 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

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.

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 under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI 2012/1500) which came into force on 1 November 2012. It restricts Authorising Officers in a local authority in England or Wales from authorising the carrying out of directed surveillance unless it is for the purpose of preventing or detecting a criminal offence and meets the following conditions:

- **that the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment; or**

- **constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old) or section 92 Children and Families Act 2014 (sale of nicotine inhaling products to children under 18 years old) or proxy purchasing of tobacco, including nicotine inhaling products, to children under 18 years old under section 91 Children and Families Act 2014.**

It is therefore essential that Investigating officers consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance

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 paragraph 2.4).

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 paragraphs 2.6 -2.10) 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 paragraph 2.5]

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 paragraphs 3.1 to 3.12)

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).

11. Authorising Officer's Statement

12. Authorising Officer's comments

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

Annex 5 - Guidance on completing Covert Human Intelligence forms

1. Details of Application

Authority Required

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

Where a vulnerable individual or juvenile source is to be used, the authorisation MUST be given by Chief Executive or in her absence the Chief Officer.

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 the use or conduct of a CHIS are 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.

6. Explain why this conduct or use of the source is necessary on the grounds you have identified (Code para 2.4)

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 to proceed.

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable (Code paras 2.6 -2.10)

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 2.9)

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 2.9)

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 paragraph 2.5]

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 paras 3.1 to 3.12). 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).

12. 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.

Annex 6 – Guidance on accessing Communications Data

[Any application for communications data (the who, when and where of a communication) must be completed on the CycComms data workflow system on the National Anti- fraud Network website at www.nafn.gov.uk. CycComms is an automated process which will enable you to apply for information, receive responses and manage your application. The National Anti-fraud Network SPoC, will act as a gatekeeper for your application, ensuring that it is practical and lawful and will engage with you to proactively provide advice~~, support and the most appropriate route which may require judicial approval. If it meets the legal threshold for obtaining communcations data NAFN will post it on the website for approval by the appropriate Designated Person~~ and support before passing to the Office for Data Communications Authorisations (OCDA). ..

This procedure necessitates the applicant to be registered with the National Anti-fraud Network prior to making the application. For details on how to do this the applicant should visit www.nafn.gov.uk.

If rejected by the ~~Designated Person~~ OCDA , NAFN will retain the application and inform the applicant in writing of the reason(s) for its rejection.

Comprehensive guidance on the application process is also available via the National Anti-fraud Network website at www.nafn.gov.uk]

1 - 7. Details of Applicant etc

Details of requesting officer's Department, Grade and contact details should be entered. The unique reference number at 4 would normally be entered by NAFN.

8. Statutory Purpose

The ONLY grounds for accessing communications data is for the purpose of preventing or detecting crime.

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.

9. Communications Data

Describe the communications data, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s).

Indicate the time periods within which the data is required. For example subscriber details can change over relatively short periods of time. Also billing data can be expensive to retrieve and should only be requested for times relevant to the investigation. It is therefore important to be specific as to the relevant time otherwise there may be collateral intrusion, the data obtained may not be relevant or the cost may be prohibitive. Times should be specified as GMT or BST. If unsure as to whether the data can be obtained from a Communications Service Provider (CSP) NAFN should be consulted.

10. Necessity

Outline brief details of the investigation, the circumstances leading to the application, the link between the communications data and the subject under investigation, the source of the data and how this data links to the offence or subject under investigation.

11. Proportionality

Explain what you expect to achieve by obtaining the requested data; what will be done with the data; how it will benefit the investigation and how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. Also explain why the specific date/timescale has been requested and how this is proportionate to what is trying to be achieved.

12. Collateral Intrusion

Collateral intrusion is intrusion into the privacy of innocent third parties. It is important to detail any plan to minimise collateral intrusion. If the subject has been contacted via the communication service (e.g. telephone number or e-mail) or if it has been used in business correspondence, advertising etc this should be explained as this demonstrates that it is being used by the subject and is therefore unlikely to result in collateral intrusion. Explain how data obtained which refers to third parties will be handled.

13. Timescale

Indicate whether the application is urgent. The Code of Practice requires CSPs to disclose the data within ten working days (an authorisation or notice will remain valid for one month unless cancelled or renewed).

Annex 7 – Guidance on Management of Covert Human Intelligence Sources

The Covert Human Intelligence Sources Code of Practice can be found on the Government website:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

1. Tasking

1.1 Tasking is the assignment given to the CHIS (i.e. to obtain, provide access to or disclose information). Where the CHIS's task involves establishing or maintaining a personal or other relationship for a covert purpose, authorisation for the use of the CHIS should be obtained in advance.

1.2 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If the nature of the task changes significantly, then a new authorisation may need to be sought.

1.3 In the event of any unforeseen action or undertakings during the task, these must be recorded as soon as practicable after the event. If the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

1.4 Where it is intended to task a CHIS in a significantly greater or different way than previously identified, the Handler and the Controller must refer the proposed tasking to the Authorising Officer and the details of such referrals must be recorded. The Authorising Officer should consider whether the existing authorisation is sufficient or needs to be replaced, which must be done in advance of any tasking.

2. Handlers and controllers

2.1 For each authorised CHIS surveillance, the Authorising Officer shall appoint an appropriate officer of the Authority ('the Handler') to have day to day responsibility for:

- Dealing with the CHIS;
- Directing the day to day activities of the CHIS;
- Recording the information supplied by the CHIS; and
- Monitoring the CHIS's security and welfare.

2.2 For each authorised CHIS surveillance, the Authorising Officer shall appoint an appropriate officer of the Authority ('the Controller') to be responsible for the management and supervision of the Handler and general oversight of the use of the CHIS.

3. Joint working

3.1 There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. For example, where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/ local authority anti-social behaviour operation on a housing estate.

3.2 In the event of a joint activity, agreements with the other authority must be set out in writing.

4. Security and Welfare

4.1 Prior to authorising the use or conduct of CHIS, the Authorising Officer should be satisfied that a risk assessment has been carried out. The risk assessment should determine the risk to the CHIS of any tasking and the likely consequences should their identity become known; and should consider the ongoing security and welfare of the CHIS after the cancellation of the authorisation. ,Consideration should also be given to the management of any requirement to disclose information tending to reveal the existence or identity to, or in court.

4.2 The Handler is responsible for bringing to the attention of the Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

Annex 8 – ESCC Internal Guidance concerning Applications for use of Covert Investigative Techniques

East Sussex County Council
Internal Guidance concerning Applications ~~under RIPA~~ for use of Covert Investigative Techniques

Introduction

This guidance is given for any person who is considering the use of the following in the course of their work:-

- Directed Covert Surveillance
- ~~Access to Communications Data~~
- Use of Covert Human Intelligence Sources (CHIS)

This should be read in conjunction with the ESCC Policy in ~~respect of~~ RIPA relation to the use of Covert Investigative Techniques and any associated guidance provided by Government. This internal guidance seeks to complement the policy whilst ensuring that sufficient quality control and adequate record control is maintained.

NB Applications for access to communications data shall be made via the National Anti Fraud Network (NAFN) who will then arrange for it to be submitted to the Office for Communications Data Authorisations. Guidance for use of the NAFN portal is published and updated on the NAFN website.

Key Participants

Philip Baker, Assistant Chief Executive is the Senior Responsible Officer (SRO) for covert investigatory techniques under the Regulator Investigatory Powers Act (RIPA) within the authority. As such he maintains the central record and has overall oversight.

However, on a day-to-day basis, Richard Strawson, Team Manager for Trading Standards, has been designated the RIPA Co-ordinating Officer (RCO) and will exercise oversight and quality control within the authority.

A list of Authorising Officers is available on the intranet, and any person listed will be able to authorise appropriate RIPA activity, subject to the necessary judicial authorisation.
If an Officer is considering an application the RCO may be contacted to offer initial guidance and support.

Applications

The following process must be followed in the case of all applications.

1. The Applicant should familiarise themselves with the RIPA Policy, Home Office Guidance and the relevant application form.
2. The Applicant must contact the RCO who will discuss the validity of the proposed application and offer any guidance prior to making an entry on the Central Record and allocating a Unique Reference Number (URN) for use on the application form.
3. The Applicant should write the application by hand and submit it, together with all relevant supporting information and intelligence, to one of the designated Authorising Officers.

4. The Authorising Officer will consider the application and if deemed sufficient complete the authorisation, notifying the RCO that he/she has done so in order for the Central Record to be updated.
5. The Applicant must contact the Magistrates' Court in order to arrange for Judicial Approval.
6. The Applicant should attend the hearing with, if deemed appropriate, the Authorising Officer.
7. Once Judicial Approval is obtained, the Applicant must take a working copy of the application and the original application and signed Judicial Approval returned to the RCO who will arrange for the Central Record to be updated.
8. The Applicant and Authorising Officer are to liaise regarding the need for any application for renewal and any original renewal will be given to the RCO who will arrange for the Central Record to be completed.
9. The Applicant and Authorising Officer will continue to liaise, undertake reviews and cancel the authorisation. On completion of each review or cancellation document, a copy is to be retained as a working copy and the original giving to the RCO who will arrange for the Central Record to be completed.
10. The RCO will be responsible for briefing the SRO regarding the application and will discuss at quarterly briefing meetings. A summary will also be provided for inclusion in a quarterly report to Cabinet and Council.
11. The RCO will use his oversight and gate keeping function to suggest reviews and changes to policy, maintaining best practice and training, in consultation with the SRO.

Richard Strawson
Team Manager – Trading Standards
Version ~~1.2~~ 2.1, July ~~2018~~ 2020