Essex County Council

POLICY AND PROCEDURES ON COVERT SURVEILLANCE AND THE COVERT HUMAN INTELLIGENCE SOURCES

Executive Summary

This document sets out Essex County Council's policy and procedures about the use of covert surveillance and using Covert Human Intelligence Sources (informant or undercover officer). It applies to all parts of the Council.

Some activities need to be authorised under the Regulation of Investigatory Powers Act 2000 (broadly, these are investigations into alleged criminal offences).

Sometimes, for example in HR investigations, the Council will want to undertake these activities when it is not possible to authorise the activities under RIPA. This policy also deals with these activities.

ALL Covert Surveillance or use of a Covert Human Intelligence Source must be authorised by an authorising officer. Any authorisation granted under RIPA must additionally be approved by a Magistrate. All authorisations and refused applications must be recorded in the ECC central register which is held within Internal Audit. There is also a short 'Guidance Note for Officers' about RIPA and a separate policy covering acquiring of communications data.

Policy

1. Background

1.1 In order to carry out its statutory responsibilities, the Council sometimes needs to carry out investigations. Investigations may sometimes need covert surveillance or covert human intelligence sources to be used.

1.2 As a public authority the Council must respect people's human rights as set out in the European Convention on Human Rights. Article 8 of the Convention requires the state to respect people's private and family life. This is not an absolute right. The state can interfere with this right in order to prevent or detect crime or disorder. Any such interference has to be in accordance with the law.

1.3 The Regulation of Investigatory Powers Act 2000 provides a legal framework which allows the Council to undertake:

- the acquisition of communications data (e.g. billing data);
- non-intensive covert surveillance in the course of specific operations;
- the use of covert human intelligence sources (agents, informants, undercover officials).

1.4 The Act sets out a legal process. If the process is followed, these activities are 'in accordance with the law'. The Council's use of investigatory powers is regulated by the Investigatory Powers Commissioners Office (IPCO).

1.5 There is a separate policy document in ECC which relates to acquisition of communications data.

2. Record Keeping

2.1 Record keeping is important to demonstrate compliance with RIPA. Each service maintains a local record. A central record is maintained by the Monitoring Officer.

2.2 The Council also maintains a central record of technical equipment used for directed surveillance.

3. Codes of Practice

3.1 The Secretary of State has issued Codes of Practice for directed surveillance and the use of CHIS.

3.2 More about the legislation and the codes of practice are to be found on gov.uk at this link

4. Roles

4.1 This policy defines four roles in the authorisation process.

4.2 **Applicants:** Anyone may apply for a RIPA or non RIPA authorisation.

4.3 **Authorising Officers:** Authorisations may be approved only by those named at appendix 1. Once approved the application must then be approved by a Magistrate.

4.4 **Senior Responsible Officer** ('SRO') who is responsible for compliance, the integrity and management of the process to minimize the risk of errors, including oversight and reporting of any errors to the IPCO, and liaison with the Commissioner. The Senior Responsible Officer is the Director, Legal and Assurance.

4.5 **Co-ordinating Officer:** Responsible for maintaining the central record on behalf of the SRO. The Co-ordinating officer is the Counter-fraud Manager.

5. Joint Working and use of Contractors

5.1 Where the Council works jointly with another investigating agency, either organisation may obtain RIPA authorisations. The lead organisation must ensure that RIPA compliance has been secured.

5.2 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not public authorities (such as a non-governmental organisation, company, individual or private detective). Where that third party is working in partnership or under the direction of the Council then they are working as an agent of the Council. Any act that the third party conducts should be considered for authorisation, particularly if the Council wishes to make use of any material obtained.

5.3 Anyone working on the investigation must see a copy of the authorisation (or at least the relevant parts of it) so that they know what has been authorised.

54 Where ECC staff undertake activities authorised by an authorisation which wasn't granted by the Council, a copy of the authority of the other agency must be retained and recorded on ECC's central register.

6. Surveillance Board

6.1 The Surveillance Board is chaired by the Senior Responsible Officer and there are representatives from all directorates. The Surveillance Board has the following terms of reference:

1. To have oversight of appropriate arrangements for authorising and carrying out surveillance including covert directed surveillance, use of covert human information sources, prosecutions relating to recovery of proceeds of crime and use of cctv/ vehicle number plate recognition cameras.
2. To review the following policy as required and at least annually: Operational Policy and Procedural Guidance on the Use of Covert Surveillance and the Use of Covert Human Intelligence Sources.
3. To react to reports or audits that relate to surveillance and to ensure that recommendations of the Office of Surveillance Commissioners are implemented.
4. To ensure that a training programme is in place for officers involved in surveillance.
5. To ensure that officers who need to be are aware of the existence of the policy and are able to access it.
6. To monitor that the Council keeps accurate and up to date records as required.
7. To report to Audit, Governance and Standards Committee annually with statistics and to ensure that the Audit, Governance and Standards Committee reviews the surveillance policy at least annually.

7. Member Involvement

7.1 The Code of Practice recommends that members are involved in review of this policy at least annually, and that statistical information about RIPA authorisation is provided to members at least quarterly. At Essex the Audit, Governance and Standards Committee has oversight of this issue. The Co-ordinating Officer is responsible for reporting to the committee in relation to the annual review and provision of statistics.

8. Use of material as evidence in court proceedings

8.1 Subject to the usual rules of evidence, material obtained through covert surveillance (or through a CHIS) may be used as evidence.

8.2 Material obtained through surveillance or the use of a CHIS is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996. There are legal procedures which can protect the identity of a CHIS from disclosure.

9. Covert surveillance of Employees etc outside RIPA

9.1 The Investigatory Powers Tribunal[1] has decided that RIPA authorisations may only be granted when an organisation is carrying out its core functions, and not when it

[1] C and (1) THE POLICE (2) HOME SECRETARY
DEPARTMENT 14 November 2006 No: IPT/03/32/H

is acting as employer. However, surveillance of employees may still potentially be viewed as infringing their article 8 rights.

9.2 Where surveillance relating to a matter which is either not an offence or where prosecution does not form part of the Council's core business is required, officers are required to complete the appropriate form (headed 'Non-RIPA Authorisation')and seek appropriate internal authorisation. One example of this would be if the Council seeks to undertake surveillance on employees as part of a disciplinary case. Non-RIPA authorisations will last for 3 months and appropriate action must be taken to review, renew and cancel authorisations.

9.3 The authorising officers will apply the same tests of necessity and proportionality for non-RIPA authorisations as would apply to RIPA authorisations.

9.4 Magistrates have no role in approval of 'non-RIPA' activities.

9.5 Once internally authorised, a signed copy of the authorised form and subsequent review, renewal and cancellation forms must be kept secure with the investigation file and with the central record maintained by the Co-ordinating Officer.

10. Forms

10.1 The Council has adopted Home Office forms. These are available on the Internet at this link 10.2. Forms for 'non RIPA' authorisations (e.g. HR investigations) are available on the intranet.

Essex Procedures and Complying with Codes of Practice.

This part of the document is divided into two sections.

Section A is concerned with directed covert surveillance, including intrusive surveillance, Section B with the use and conduct of covert human intelligence sources.

Section A - Covert Surveillance

11. Surveillance definitions and when RIPA authority can be granted.

What is meant by 'covert surveillance', 'directed surveillance' and 'intrusive surveillance'?

11.1 **Surveillance** includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications.

11.2 **Covert surveillance** is any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place (section 26(9)(a)).

11.3 **Directed surveillance** is surveillance which is covert, but not intrusive, and undertaken for the purposes of a specific investigation or specific operation; in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) (section 26(2)).

11.4 The Council can only use RIPA authorised surveillance for the detection or

prevention of 'serious crime'. This means offences which carry a maximum sentence of at least 6 months imprisonment or relate to the sale of alcohol or tobacco to children.

11.5 Surveillance which is an immediate response to events is outside the provisions of RIPA. There is no requirement to follow the RIPA procedures in these circumstances.

11.6 **Intrusive surveillance** is surveillance which takes place on residential premises or in private vehicles. The Council **cannot** authorise the use of 'intrusive surveillance'. Where such activity is considered necessary to prevent or detect a crime, the matter should be referred to the Police.

11.7 General observations form part of the duties of many law enforcement officers within public bodies. For example, Trading Standards officers may covertly observe and then visit a shop as part of their enforcement function. They may observe goods or services being supplied. Such observation may involve the use of equipment to reinforce normal sensory perception such as binoculars or cameras. Such activity forms part of the everyday function of law enforcement officers within public bodies. This is considered to be low-level activity, which will not usually be regulated under RIPA. Similarly, plain clothes operations, even if targeted at a particular area, are not directed surveillance and are not required to be authorised.

11.8 If one or more particular individuals are being targeted as part of an operation, and private information about them is likely to be obtained during the operation, then RIPA authority should be obtained.

Use of Public CCTV Systems

11.9 General use of public space CCTV systems is overt and therefore not covered by RIPA. If one or more CCTV cameras are targeted on an individual then this may be directed surveillance which must be authorised under RIPA.

Social Media and Internet Based Research

11.10 Reading someone's public postings on social media may not feel like an interference with someone's human rights. However, the compilation of a file information on somebody by the state has been held to be an interference with the human right to respect for privacy.

11.11 The law is the same for any collating any information about individuals. Viewing social media postings which are available to the public is the same as cutting an article out of a newspaper or putting other information on a file.

11.12 Any such activity needs to be 'in accordance with the law'. Any building up of information on a file about someone needs to be undertaken in accordance with the General Data Protection Regulation and the Data Protection Act 2018.

11.13 However, RIPA applies only where the Council undertakes activities which are covert – ie they are intentionally undertaken in such a way that the subject doesn't know it is taking place, and the activity is likely to result in the obtaining of private information. When viewing open postings on social media, you must not do so in a covert way unless it is authorised by RIPA. Repeated viewing of a social media profile could amount to covert surveillance if undertaken covertly and it is wise to

keep this to a minimum.

11.14 It would normally be covert to form a formal online 'friendship' to view closed information (eg follow someone who protects their tweets or view a facebook profile which is not public). Any use of this must be carefully considered as this could amount to directed surveillance or the use of a 'covert human intelligence source' which would need to be authorised under RIPA.

11.15If you are intending to make social media checks then you should consider notifying the subject first. . You do not have to do this if it would prejudice prevention or detection of crime to do so. If you have notified someone that you will be making checks then the viewing of social media is not covert and does not need to be authorized.

11.16 As with any personal data held by the Council we need to ensure that we comply with the General Data Protection Regulation and Data Protection Act 2018. That is beyond the remit of this policy but advice is available from Information Governance or Essex Legal Services .

11.17 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information (see above for more information about private information) about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile as part of a covert operation;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

12. Obtaining Authority for Directed Surveillance

12.1 An applicant must complete the application and submit it to an authorising officer. The form must be carefully completed and should not use standard wording in the boxes of the form. The authorising officer must consider the application and, if they

grant the authorisation they must use their own words to explain their decision and say what is authorised. They must ensure that the activity is necessary and proportionate and define the parameters of the permitted activity. Even when the authorising officer has approved the authorisation, the authorisation does not take effect unless and until it is approved by a Magistrate.

12.2 The proposed surveillance must be planned in connection with an investigation for one of the Council's core statutory functions (eg trading standards).

12.3 A written application for authorisation for directed surveillance should describe any conduct to be authorised and the purpose of the investigation or operation. The application should be fair and balanced and include:

- the reasons why the authorisation is necessary in the particular case for the purpose of preventing or detecting a serious crime (or other reason may be possible in relation to a 'non RIPA' authorisation)
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance, including automated online search engines (the extent and limitations should be considered and detailed);
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- an assessment of the risk of collateral intrusion and details of the measures taken to minimize the risk;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

12.4 All authorisations must be issued in writing. All reasonable efforts should be made to take account of information which supports or weakens the case for authorisation.

12.5 Once an authorisation is approved, the authorisation must be referred to a Magistrate for approval (except for non-RIPA authorisations - which should not be referred to the Magistrate).

12.6 An application for approval by a Magistrate will be made:

(a) by an officer approved by the Trading Standards Manager or
(b) by an officer approved by the SRO

If the Magistrate does not approve the authorisation at the first hearing then, in all cases, the SRO must be informed as a matter of urgency.

In all cases the SRO must be informed of the date and time of the magistrates' decision and provide details of the hearing for the central record – see paragraph 17.2.

12.7 A flowchart explaining the Magistrate Approval process is at this link

12.8 A record of the Magistrate's Decision must be sent to the Co-ordinating Officer.

13. Necessity and Proportionality

13.1 The Council can only use RIPA powers if it is necessary and proportionate to do so.

13.2 The applicant must explain why they believe the proposed activities are necessary and proportionate. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it, against the need for the activity. It will always involve explaining why this is the least intrusive way possible, and presented in a fair and balanced way.

13.3 The activity will not be proportionate if the information which is sought could reasonably be obtained by other less intrusive means or if the intrusion is significant compared to the matter being investigated.

14. Collateral Intrusion

14.1 Collateral intrusion refers to activities where information is obtained about people other than those who are directly the subject of the investigation or operation. The risk of collateral intrusion must be assessed as part of proportionality. Wherever practical, measures should be taken to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

14.2 Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

14.3 Before making an application the applicant should consider whether there are particular sensitivities in the local community where the surveillance is taking place which should influence the grant.

15. Confidential Information

15.1 The RIPA code of practice suggests that particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. ECC officers are unlikely to come into possession of information of this nature, but need to be alert to the correct procedures should such a situation arise.

15.2 If it is likely that confidential information will be acquired, the use of surveillance must be authorised by the Chief Executive or in his absence the Monitoring Officer.

15.3 Legally privileged information is confidential information. It is unlikely that surveillance will result in legally privileged information being obtained. Any such information is extremely unlikely ever to be admissible as evidence in criminal proceedings and the Council would not seek to acquire such material.

15.4 An application for surveillance likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances.

16. Combined authorisations

16.1 The Code of Practice states that a single authorisation may combine two or more different RIPA authorisations. For example, a single authorisation may combine authorisations for directed surveillance and the conduct of a CHIS. In such cases the provisions applicable to each of the authorisations must be considered separately. However as the application forms would need to be separately completed and the criteria involved in both is different, it is recommended that the authorisations are considered separately. Authorisations covering directed surveillance at multiple sites (eg undertaking surveillance of a number of premises as part of test purchasing operations) are appropriate.

17. Central Record

17.1 In accordance with the codes of practice the Council keeps a centrally retrievable record of all authorisations which is regularly updated whenever an authorisation is refused, granted, renewed or cancelled. These records will be retained for a period of at least three years from the ending of the authorisation.

17.2 The following information will be kept on the central record: -

- the type of authorisation
- the time and date the authorisation was given or refused and the date upon which it was notified and approved by a magistrate;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- details of the attendances at the Magistrates' court, to include the date of attendance, he determining magistrate, the decision of the court and the time and date of the decision;
- the dates of any reviews;
- dates of any renewals and the name and rank/grade of the authorising officer;
- the result of periodic reviews of the authorisation;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in the code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled;
- a record of all Magistrate decisions, including reasons for any refusals, where applicable and details of any appeal to the Investigatory Powers Commissioner.

17.3 The following documents will be kept with the central record:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- date and time when any instruction was given by the authorising officer

- Magistrate decisions;
- the date and time when any instruction to cease surveillance was given.

17.4 The Co-ordinating Officer maintains records on behalf of the Senior Responsible Officer.

17.5 A central record is also kept of the technical equipment used by the Council for covert surveillance. Any officers or services making use of equipment for covert surveillance should ensure that details are passed to the Co-ordinating officer to be added to the register.

18. Duration of Authorisations

18.1 A written authorisation granted by an authorising officer and approved by a Magistrate will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the date of approval by the Magistrate.

18.2 Surveillance must only be undertaken in accordance with the terms of the authorisation. If anyone concerned in the operation is concerned that there may be an error which has resulted in unauthorised directed surveillance taking place

19. Reviews

19.1 The authorising officer will specify a frequency of reviews when they complete the authorisation. It is suggested that this is monthly but the frequency will depend on the circumstances. The relevant review form must be completed on each occasion and a copy sent to the Co-ordinating Officer. The review must be signed by an authorising officer but does not need to be approved by a Magistrate. The results of the review must be retained for at least 3 years.

20. Renewals

20.1 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of **three months**.

20.2 Renewals must be approved by a Magistrate using the same procedure as the original authorisation.

20.3 A renewal takes effect at the time at which, or day on 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 is 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.

20.4 Applications for the renewal of an authorisation for directed surveillance should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the circumstances or information detailed in the initial application;
- the reasons why it is necessary to continue with the directed surveillance;

- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- whether any privileged material or confidential information was obtained as a result of the activity undertaken under the authorisation;
- the results of regular reviews of the investigation or operation.

20.5 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations. All renewals must be approved by a Magistrate.

21. Cancellations

21.1 The authorisation must be kept under review and be cancelled by an authorising officer (usually the officer who granted or last renewed it) if the criteria upon which it was authorised are no longer met or if the authorisation is no longer required.

21.2 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central record of and the notification of cancellation where relevant.

22. Errors

22.1 The Council expects authorising officers to carefully applications before approving them and any application is reviewed by the person presenting the application to a Magistrate, reducing the risk of errors. However, all 'relevant errors' must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, but no later than 10 working days after it has been established that a relevant error has occurred. The report should include as much detail regarding how the error occurred, the impact of the error and what steps are being taken to prevent any recurrence

22.2 A relevant errors is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Commissioner. These include the following:

- Activity has taken place without lawful authorisation;
- There has been a failure to adhere to the safeguards regarding the handling of any material gained under a statutory authorisation.

22.3 Section 231 of the 2016 Act requires the Investigatory Powers Commissioner to inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious nature and it is in the public interest for the person concerned to be informed of the error.

22.4 In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must consider:

- The seriousness of the error and its effect on the person concerned
- The extent to which disclosing the error would be contrary to the public interest or prejudicial to:
    - National security
    - The prevention or detection of serious crime
    - The economic well-being of the UK; or
    - The continued discharge of the functions of any of the intelligence services.

22.5 If it identified that an error **may** have occurred the Senior Responsible Officer must be informed immediately by email or telephone. The Senior Responsible Officer will ensure that prompt action is taken to establish what has occurred and whether or not this is an error which must be reported to the Commissioner. A record will be made of any decision taken and the reasons for it,

23. Retention and destruction of the product

23.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained securely. The Criminal Procedure and Investigations Act 1996 requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

23.2 There is nothing in RIPA that prevents material obtained from properly authorised surveillance from being used in other investigations.

23.3 Officers must ensure that arrangements are in place for the handling, secure storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements.

Guidance on Use of Covert Human Intelligence Sources and RIPA

24. What is a Covert Human Intelligence Source?

24.1 A person is a covert human intelligence source ('CHIS') if he or she establishes or maintains a personal or other relationship for the covert purpose of obtaining information or to provide access to any information to any other person or he or she secretly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. A CHIS may be an informant - or an officer working undercover.

24.2 Officers should be aware that there is a risk of someone becoming a CHIS if they give the Council information on more than one occasion if that information comes from a relationship they are maintaining if it can be said that they are partly maintaining the relationship for a covert purpose.

24.3 This can happen almost by inadvertence. If someone becomes a CHIS then use of this policy should be considered.

25. When may the Council use a CHIS?

25.1 There may be occasions when it is appropriate for an ECC officer to be authorised as a CHIS. However, should the use of a third party, non-ECC officer CHIS become necessary to ensure effective law enforcement, appropriate arrangements must be made with Essex Police to carry out this function on behalf of the Council.

25.2 The routine making of simple test-purchases is not usually considered to require a CHIS authorisation. However, if a continuing relationship (whether personal or business) is formed then test purchases may need to be considered for authorisation. Simple test purchases watched by officers involve directed

surveillance and not use of a CHIS.

25.3 Forming an online 'friendship' on Social Media in order to view closed postings (eg follow someone who protects their tweets or view a facebook profile which is not public) must be carefully considered. This could amount to directed surveillance or the use of a 'covert human intelligence source' which would need to be authorised under RIPA.

26. When is a relationship covert?

26.1 A relationship is used covertly if it is conducted in a manner calculated to ensure that one party is unaware of its purpose.

27. What safeguards must the Council observe before using human intelligence sources?

27.1 The Council must be satisfied:-

- That use of a CHIS is in connection with the Council's statutory functions.
- That use of a CHIS is likely to impact on someone's human rights, for example the right to respect for private and family life, home and correspondence, that such interference is proportionate and can be justified.
- That use of a CHIS is properly authorised and lawful.

27.2 Only authorised officers listed in Appendix 1 may grant an authorisation.

27.3 Following the internal authorisation process the decision must be referred to a Magistrate for approval.

28. Authorisation of a CHIS

28.1 An authorisation approved by a Magistrate under Part II of RIPA will provide lawful authority for the County Council to use a CHIS.

28.2 Officers involved in the use of CHIS should refer to the statutory Code of Practice.

28.3 Local authority staff may only grant authorisations if the activities are necessary for the purpose of preventing and detecting crime or of preventing disorder. Note that the 'serious crime' threshold (as set out in paragraph 11.3) which applies to directed surveillance does not apply to the use of a CHIS.

29. Necessity and Proportionality

29.1 RIPA requires that the person granting an authorisation believes that the use of the source is necessary and proportionate.

29.2 Use of the source is necessary if the Council needs the information as part of the investigation it is undertaking. It is proportionate if the benefit of the source outweighs the intrusion. To assess this a balancing exercise must be undertaken weighing up the intrusion with the benefit of using the source. This involves considering whether the information which is sought could reasonably be obtained by other less intrusive means.

29.3 The use of a source should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

30 Collateral Intrusion

30.1 An application for an authorisation should include an assessment of the risk of 'collateral intrusion' – ie intrusion into the privacy of anyone who is not directly the subject of the investigation or operation. This includes passers-by or the family of the person who is under investigation. See section 14 for more information.

31. Vulnerable Adults

31.1 A vulnerable individual should only be authorised to act as a source in the most exceptional circumstances. You should refer to the code and take legal advice before proceeding.

31.2 A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

32. Juvenile sources

32.1 Special safeguards also apply to the use or conduct of sources under the age of 18. **Authorisations should not be granted to use a source under 16 years of age to give information against a parent**. Authorisations should not be granted with respect to a young person unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2002/793) are satisfied. The duration of such an authorisation is **four months** instead of twelve months.

32.2 The use of young people by ECC Trading Standards to make routine, simple underage test purchases of age-restricted goods is not considered to be the use of a CHIS. However, each case will be considered on its merits and if a proposed operation might involve formation of a relationship with the seller, an application for the appropriate authorisation should be made.

33. Authorisation Procedures for CHIS.

33.1 Under s29(3) of RIPA an authorisation for the use or conduct of a source may be granted by an authorising officer where he believes that the authorisation is necessary in the circumstances of the particular case for the purpose of preventing and detecting crime or of preventing disorder.

33.2 The Council makes very sparing CHIS authorisation powers. Detailed guidance has not been included in these notes. Reference should be made to the procedure for authorising directed surveillance. See also the flow chart relating to Magistrates' Approval in the Home Office Document at this link.

33.3 Authorisation for the use of a CHIS will, unless renewed, cease to have effect at the end of a period of **twelve months** beginning with the day on which it was approved by a Magistrate.

33.4 Regular reviews of authorisations should be undertaken to assess the need for the use of the source to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the use of a source provides access to confidential information or involves collateral intrusion.

33.5 Authorisations should be renewed unless there has been a recent review.

33.6 A renewal takes effect at the time at which, or day on 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, if necessary, provided they continue to meet the criteria for authorisation. The renewal should be kept/recorded as part of the authorisation record.

33.7 Any renewal must also be approved by a Magistrate.

33.8 All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the
- authorisation has been renewed previously;
- any significant changes to the information provided on the original application or any previous reviews;
- the reasons why it is necessary to continue to use the source;
- the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation;
- the tasks given to the source during that period and the information obtained from the conduct or use of the source;
- the results of regular reviews of the use of the source;

34. Cancellations

34.1 The authorisation should be cancelled, usually by the officer who granted or renewed the authorisation if he is satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that satisfactory arrangements for the source's case no longer exist, or if the use of the CHIS is no longer required.

34.2 Where necessary, the safety and welfare of the source should continue to be considered after the authorisation has been cancelled.

35. Management of Sources

35.1 The Code of Practice should be followed about management of the source.

35.2 In particular you should note the requirement for two senior officers to be involved in the management of the CHIS.

One person must have day to day responsibility for:

- dealing with the source on behalf of the authority concerned;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare;

Another person must have general oversight of the use of the source.

35.3 The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.

35.4 In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

35.5 ECC will consider safety and welfare when carrying out actions in relation to authorisation or tasking, and to foreseeable consequences to others of that tasking. A risk assessment must be carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known before authorising the use or conduct of a source. The long term security and welfare of the source should also be considered at the outset.

36 Combined authorisations

36.1 A single authorisation may combine two or more different authorisations under Part II of RIPA (eg authorising CHIS in connection with test purchases at more than one venue). It is not appropriate to have a single form dealing with applications for surveillance and a CHIS in the same form.

37 Central Record of all authorisations

37.1 In accordance with the codes of practice a centrally retrievable record of all authorisations is kept by the County Council and updated whenever an authorisation is granted, renewed or cancelled. Records are retained for three years from the end of the authorisation.

37.2 The following information and documents will be kept on the central record:-

- a copy of the authorisation
- a copy of any decision taken by a magistrate;
- a copy of any renewal or review of an authorisation;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the authorising officer to cease using a source.

37.3 The SRO is responsible for overseeing compliance with RIPA. The central records are kept under the supervision of the SRO. Copies of each document listed above must be sent to the Co-ordinating Officer immediately.

38 Retention and destruction of the product

38.1 Where the product obtained from a source could be relevant to pending or future

criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review. Particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

38.2 There is nothing in RIPA which prevents material obtained from properly authorised use of a source from being used in other investigations.

38.3 Officers must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. This includes compliance with the data protection principles which require data to be kept securely and to be destroyed when no longer required for the original purpose.

39. Errors.

39.1 Section 24 of this document applies to errors in the use of a CHIS in the same way as it applies to directed surveillance.

APPENDIX 1

Senior Responsible Officer

Director, Legal and Assurance – Paul Turner

Authorising Officers

The following officers are authorised to act as authorising officers for the purposes of an application for an authorisation to carry out directed surveillance and for the use or conduct of a covert human intelligence source.

The Head of the Paid Service – Gavin Jones
Service Manager for Trading Standards – Matthew Sanctuary
Head of Assurance – Paula Clowes
Where confidential information is likely to be acquired, authority must be obtained from the Head of the Paid Service or in their absence the Monitoring Officer.

Where there is an allegation of fraud or corruption the Head of Assurance must be notified and agree to any surveillance which is not under his/her direct control.

Co-ordinating Officer

Karen Bellamy – Counter Fraud Manager, Legal and Assurance

Advice on RIPA

Advice on the use of RIPA is available from the SRO, the Service Manager for Trading Standards or Essex Legal Services.

Record Keeping

Information for the Central Record should be sent to the Co-ordinating Officer.

Version control

Amended policy effective from June 2017.

Title	OPERATIONAL POLICY AND PROCEDURAL GUIDANCE ON THE USE OF COVERT SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES
Author/Owner	Owner: Director – Legal and Assurance
Status	
Version	
Date	June 2017
Review date	2018
Security classification	Not protectively marked
Approved by	Full version approved by Audit, Governance and Standards Committee. Name changed approved by Director, Legal