REGULATION OF INVESTIGATORY POWERS

POLICY AND PROCEDURE

BasildonCouncil
BASILDON • BILLERICAY • WICKFORD

Creating Opportunity, Improving Lives

Key Information (To correspond with Covalent)

Author:	Rachel Glover (Environmental Health Services Manager) Lyndsey Smith (Assistant Solicitor)
Section/Directorate:	Public Spaces
Service Impact Assessment:	3 June 2019
External Consultation:	None
Internal Consultation:	Audit and Risk Committee (26 June 2019) Internal RIPA Working Group Assurance and Governance Board (11 June 2019)
Background Information:	Regulation of Investigatory Powers Act 2000, as amended, together with associated Orders and Codes of Practice.
Policy Approval – Officer Level	Service Director (RIPA 'Senior Responsible Officer')
Policy Approval – Member Level	Audit and Risk Committee – 26 June 2019
Policy Review Date:	June 2022
Service Impact Assessment Review Date:	June 2022

Content

1. Introduction

1.1 Basildon Borough Council ("the Council") is allowed, and required, to carry out investigations in relation to its duties. Such investigations may require surveillance or information gathering and this is often undertaken overtly, meaning the person being investigated is fully aware of the situation. This type of surveillance is not the subject of this policy and does not require authorisation. In some circumstances, it is necessary to undertake surveillance or information gathering in a covert manner, meaning the individual is not made aware of such activity. The purpose of this policy is to ensure there is a consistent approach to the undertaking and authorisation of such surveillance activity.

1.2 The Regulation of Investigatory Powers Act 2000 (RIPA), has far reaching implications for many areas of work carried out by the Council. This document sets out the principles to be taken into consideration when authorising and/or seeking to carry out covert surveillance activity. The purpose of this Policy is to ensure there is a consistent approach by the Council and Officers to the undertaking and authorising of surveillance activity where RIPA applies. This Policy is to be used by all Council service areas and officers undertaking investigation and using the techniques of surveillance and/or the use of Covert Human Intelligence Sources (CHIS's).

1.3 Since the policy was first adopted, changes have been made to ensure compliance both with the recommendations of Internal Audit review and of inspections by the Office of the Surveillance Commissioner (who has more recently become the Investigatory Powers Commissioner's Office (IPCO)). The Council's RIPA Working Group monitors the use of covert techniques and any changes in legislation and good practice. This Policy has been updated as necessary to reflect changes to legislation and Home Office Codes of Practice.

1.4 The codes of practice assist public authorities to assess and understand whether, and in what circumstances, it is appropriate to use covert techniques. The codes also provide guidance on what procedures need to be followed in each case. The current codes of practice are:

(i) Interception of communications
(ii) Equipment Interference
(iii) Acquisition, Disclosure and Retention of Communications Data
(iv) Covert Surveillance
(v) Covert Human Intelligence Sources
(vi) Investigation of Protected Electronic Information.

1.5 Following decisions made by the Audit and Risk Committee and Cabinet in 2010, a role was established for elected Members to scrutinise the authority's compliance with RIPA and relevant codes of practice. (NOTE: Refer to paragraph 8 of this policy for more details of the role of councillors).

2. Executive Summary

2.1 The Regulation of Investigatory Powers Act regulates the way in which the Council conducts surveillance for the purposes of law enforcement. The fundamental requirement of RIPA is that when the Council considers undertaking directed surveillance or using a covert human intelligence source, it must only do so if:

a) The activity has been authorised by an officer with appropriate powers, and
b) The relevant criteria are satisfied and that in relation to directed surveillance the alleged offences carry a minimum sentence of six months imprisonment, and that confirmation of approval has been given by a Magistrate.

2.2 This policy sets out the Council's approach to covert surveillance and the use of covert human intelligence sources. In particular, it details the checks and balances in place to ensure that any use of covert techniques is lawful, necessary and proportionate.

3. Policy Statement

3.1 Basildon Council takes its statutory responsibilities seriously. The Council is committed to carrying out its duties in relation to its investigation and enforcement activities in a lawful manner. It recognises the importance of ensuring necessary and proportionate action is taken where offences may be being committed, but that this action also needs to consider the rights of an individual and the protections which the Human Rights Act 1998 may bring. This policy particularly relates to directed surveillance, the use of a Covert Human Intelligence Source (CHIS) or acquisition of communication data.

3.2 It will achieve this by seeking to ensure that:

- All surveillance activity conducted by the Council has appropriate regard to the requirements of RIPA and the relevant provisions of the Human Rights Act 1998, and all applicable relevant legislation;
- Any necessary authorisations are carried out in accordance with the legislation, codes of practice and delegation arrangements for the authority;
- There are appropriate levels of organisational understanding of the powers set out in RIPA and more importantly how it expects to achieve compliance with the provisions set out therein.

3.3 In conducting covert investigations it is necessary to draw a balance between the rights of the individuals under investigation and the public interest. To achieve this, the Council will comply with both the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA), as amended. The Council will also comply with the RIPA (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, the Protection of Freedoms Act 2012 and the relevant supporting Codes of Practice provided by the Home Office including the updated 2018 Covert Surveillance Code and the Covert Human Intelligence Service Code of Practice.

4. Context

4.1 National – The key driver of the Policy is to ensure that the Council is fully compliant with RIPA. In addition, Article 8 of the Human Rights Convention advocates the right to privacy. To comply with this human right, surveillance, which potentially infringes the right to privacy, can only be done if it is carried out "in accordance with the law". The legal framework to authorise surveillance is provided through RIPA and its associated Codes of Practice.

4.2 Local – The Policy needs to reflect any changes in the legislative framework and the appropriate delegation in relation to authorised persons is also referenced in this Policy. It is essential that the Council has this Policy in place to ensure that it complies with RIPA and the Human Rights Act and that any evidence obtained as part of an investigation is

admissible in court. This Policy covers how the Council will utilise the powers available to it in compliance with RIPA and how the Council will do so whilst promoting its promises.

Serious Crime Test

4.3 Local Authorities can only authorise directed surveillance to prevent or detect crime where the criminal offence is either punishable on summary conviction or indictment by a maximum term of at least 6 months imprisonment or are related to underage sale of alcohol or tobacco.

4.4 A Local Authority cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence punishable whether on summary conviction or indictment by a maximum term of at least 6 months imprisonment.

4.5 In each case, the issues below must be considered.

- Ensure compliance with the data protection requirements and any other relevant codes of practice.

- Ensure that any confidential material obtained during the course of the surveillance is securely maintained. Confidential material includes matters subject to legal privilege, confidential personal information and confidential journalistic material.

  These terms are explained further in the Surveillance Code at paragraphs 4.27-4.31. Essentially there should be special consideration of this situation.

- Consider the impact of collateral intrusion relating to persons other than the subject of the surveillance. (See explanation at point 6.7 below).

- Assess whether the action is proportionate to what the surveillance seeks to achieve. In other words, is the objective important enough to justify the interference with a person's liberty & privacy? Is the Council trying to use a sledgehammer to crack a nut? i.e. the means should not be excessive in relation to the gravity of the mischief being investigated.

4.6 Examples of offences which meet the 'serious crime test' include:

- Benefit Fraud (Section 111A of the Social Security Administration Act 1992 and the Fraud Act 2006);
- Fly tipping;
- Some Planning offences (e.g. making false statements to obtain a Certificate of Lawful Development).

4.7 Investigating Officers must always check the applicable legislation to ensure that any proposed directed surveillance complies with the serious crime test.

4.8 The following offences are examples of offences that are not covered by the serious crime test:

- Littering;
- Dog fouling;
- Fly posting;

- Most planning offences, involving stop notices, enforcement notices, untidy site notices, planning contravention notices, breach of condition notices and tree preservation orders.

4.9 Once an authorisation for directed surveillance or a CHIS has been granted in accordance with the Council's scheme of delegation, approval will need to be obtained from a Justice of the Peace (JP). The judicial application/order form for a JP will need to be completed and an appointment arranged with the Magistrates' Court to arrange a hearing. On attendance at court the officer will need to have with them a counter signed RIPA authorisation/notice form, the judicial application/order form and any other relevant reference or supporting material.

4.10 If a Justice of the Peace refuses to approve the grant or renewal and quash the authorisation or notice then the local authority must be given at least 2 working days in which to make representations before the authorisation is quashed.

Consequences of Failure to Comply with the RIPA

4.11 Authorisation provides a lawful authority to carry out covert surveillance provided it is authorised in accordance with the Acts. However, a decision not to obtain authorisation does not automatically render the surveillance unlawful. The Acts and Codes of Practice are admissible in evidence and so whether authorisation was correctly obtained will be taken into account in any court proceedings about admissibility of evidence and/or human rights challenges.

4.12 If the Council fails to comply with RIPA it could be ordered to pay compensation either by a court or the ombudsman. An innocent party to collateral intrusion could be entitled to a considerable amount of compensation. It is also possible that evidence could be ruled inadmissible, although in general, case law indicates that this is less likely.

4.13 This policy document recommends that authorisations are always obtained in accordance with the Act, where appropriate assessments have been carried out in accordance with this document and the RIPA Codes of Practice.

4.14 An additional, and equally important reason to obtain authorisation is that surveillance carried out in accordance with an authorisation will be rendered "lawful for all purposes". This means that evidence obtained as a result of the surveillance will not be subject to questions around its admissibility if it is used in Court as part of a prosecution. This provides an important additional protection to an individual under Article 6 of the Human Rights Act 1998 in terms of protecting the rights of an individual to a fair trial.

4.15 In simple terms, where surveillance is planned with the intention of that person being unaware that the surveillance is or may be taking place a written authorisation in accordance with this policy must be obtained.

5 Responsible Officer

5.1 The Senior Responsible Officer is responsible for:

- The integrity of the processes in place within the authority to authorise directed surveillance, and the management of CHIS,
- Compliance with Part II of the Act and with the revised Codes of Practice,

- The oversight of the reporting of errors to the Commissioner together with the identification of the causes of errors and the implementation of processes to minimise the repetition of errors,
- Engagement with Commissioner and inspectors when they conduct their inspections, and, where necessary, oversight of the implementation of post-inspections action plans recommended or approved by a Judicial Commissioner, and
- Ensuring that Authorising Officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

5. 2 The Senior Responsible Officer will be a member of the corporate leadership team, and will have the status of an Authorising Officer. Within Basildon Council, the Senior Responsible Officer is the Deputy Chief Executive. The Senior Responsible Officer chairs the Council's RIPA Working Group.

5. 3 Data Controllers should be aware of the Record Keeping, Safeguarding, Handling, Dissemination, Copying, Storage and Destruction sections in the CHIS Code for dealing with private information. All of this is available in Chapter 9 (paragraphs 9.16 to 9.22), and its ideals are broadly captured within the Council's Information Management Policy which incorporates the Data Protection Act 2018 and the key principles outlined by the Information Commissioners Office. The Investigatory Powers Commissioner has the remit of providing comprehensive oversight of the use of the powers under RIPA and adherence to the practices and processes described in the Codes of Practice.

Authorising Officers – who can make a decision?

5.4 In accordance with the Council's Constitution, authorisations to carry out surveillance under RIPA may be granted by those authorised officers designated for that purpose and who are identified within the Council's approved RIPA policy as follows:

a) The following named posts to authorise Directed Surveillance, Covert Human Intelligence Sources applications and the accessing of communications data in accordance with the Regulation of Investigatory Powers Act 2000 (save for applications for Juvenile Covert Human Intelligence Sources): The Deputy Chief Executive, Head of Revenues, Benefits and Customer Services, Revenues and Benefits Manager, and the Environmental Health Services Manager.
AND
b) The Chief Executive (or a Director) only may authorise Juvenile Covert Human Intelligence Source applications.

5.5 It is important to note that it is the post, and *not* the current post holder, that is the Authorising Officer. If the holder of a post moves to a post that has not been designated as an Authorising Officer, they will no longer be able to give authorisation.

6. Surveillance

6.0.1 Surveillance is:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

- Recording anything monitored, observed or listened to in the course of surveillance; and

- Surveillance by or with the assistance of a surveillance device.

6.0.2 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and require different degrees of authorisation monitoring under RIPA. Where surveillance is planned with the intention of that person being unaware that the surveillance is or may be taking place a written authorisation in accordance with this policy must be obtained.

6.0.3 It is important to be aware that, in deciding whether or not surveillance is covert, or overt, the deciding factor is the intention of the officer carrying out the surveillance, and not the perception of the person being observed. Therefore, **if there is any intention to be covert, an authorisation must be obtained from an authorising Officer.**

6.0.4 Types of activity covered in the Policy are:

- **Directed surveillance**
    - Online Covert Activity
    - Aerial covert surveillance
    - Collateral intrusion
    - Collaborative working
    - The Serious Crime Test
    - Emergency situations

- **Covert Human Intelligence Source (CHIS)**
    - Online Covert Activity
    - Juvenile CHIS

6.1 Directed Surveillance

6.1.1 **Directed Surveillance** is defined as surveillance that is covert but not intrusive, and undertaken:-

- for the purposes of a **specific investigation or operation.**

- in such a manner as it is likely to obtain **private information about a person** (whether or not one specifically identified for the purposes of the investigation or operation);

- 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 this Part to be sought for the carrying out of the surveillance.

6.1.2 If observations are made as part of the normal duties of the person or officer involved, which may be termed as ‘general observations’ i.e. a planning officer noticing something whilst travelling around the town, is not directed surveillance requiring authorisation. He may consider that as a result of his observation, surveillance action is required. If this surveillance is carried out covertly (i.e. without the person being observed knowing it is or

may be taking place) then it is likely to be construed as directed surveillance and would require authorisation under the Acts. If the person subject to surveillance is advised that observations are to be carried out then this is not surveillance that is being done covertly and would fall outside the definition of directed surveillance.

6.1.3 Directed surveillance does not include any type of covert surveillance carried out in residential properties or in private vehicles. This is intrusive surveillance that local authorities cannot authorise. Section 3.7 of the 2018 Covert surveillance and property interference code of practice highlights specific situations that will require directed surveillance authorisations. These situations relate to the use of surveillance devices for private properties and vehicle locations, as well as the interception of communications in the course of transmission by means of a public postal service or telecommunication system. Section 3.27 of the Code of Practice provides specific advice on the use of surveillance in relation to private vehicles leased to a public authority.

6.2 Online Covert Activity

6.2.1 The use of the internet may be required to gather information prior to and or during an operation, which may amount to directed surveillance. Whenever the Council intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that it is likely to be necessary, an authorisation (combined or separate) must be sought. Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered.

6.2.2 Much of the information on the internet can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. If the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. Section 3.10 to 3.17 of the Covert surveillance and property interference code of practice provides additional guidance and examples as to when such authorisations may be appropriate. It is important that all relevant staff understand the complexities of carrying out internet research and understand the guidance provided in the CHIS codes. General observation duties of the Council do not require authorisation under RIPA, e.g. monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation. Specific examples are provided for further guidance at Section 3.33 of the Code.

6.3a Aerial covert surveillance

6.3.1 Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, the same considerations outlined previously should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude. (See also 3.36 to 3.39 of the CHIS code with regard to overt surveillance cameras.)

6.3b Intrusive Surveillance

6.3.2 Is defined as covert surveillance that:

- is carried out in relation to anything taking place on any **residential premises or in any private vehicle** (this is distinct to vehicles owned or leased by public authorities as further explained in Section 7.49 of the Code); and
- involves the **presence** of an individual on the premises or in the vehicle or is carried out by means of a surveillance devise.

6.3.3 If surveillance activity falls within the definition of intrusive surveillance, this falls outside the scope of activity which can be authorised and carried out by a local authority. It is reserved for a small number of law enforcement agencies and the intelligence services. It will also make authorisations in respect of such surveillance subject to prior approval by either an independent Judicial Commissioner (for law enforcement agencies) or the Secretary of State (for the intelligence services). (Section 3.20). The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained, as it is assumed that intrusive surveillance will always be likely to result in the obtaining of private information.

6.3.4 Intrusive surveillance does not include the use of overt CCTV cameras positioned in their normal position where the public are aware that the systems are in use for their own protections and to prevent crime. The use of overt CCTV cameras by the Council does not normally require an authorisation under the 2000 Act. However, members of the public should be made aware that such systems are in use by way of signage etc. and consideration will still need to be given to the Human Rights and Data Protection Acts (Sections 3.36 to 3.39 of the Code of Practice provides further explanation).

6.3.5 Furthermore, this does not include surveillance carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle i.e. a tracking device. This is classed as directed surveillance and would require authorisation for this in the usual way.

6.3.6 **It must be remembered that local authorities cannot authorise intrusive surveillance**. Section 3.31 of the Code of Practice explains activities not falling within the definition of covert surveillance.

6.4 Private, Confidential and Legally Privileged Information

6.4.1 The handling of information obtained by means of covert surveillance will be carried out in accordance with other relevant legal frameworks, as well as in accordance with the RIPA Codes of Practice, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including data protection controls implemented by the Council, and the requirements of the Police and Criminal Evidence Act, will ensure that the handling of private information obtained through the use of this policy, continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.

6.5 Communications Data

Local authorities are required to fulfil two additional requirements when acquiring communications data, namely:

- the request must be made through a Single Point of Contact at the National Anti-Fraud Network;
- the request must receive prior approval from the Office for Communications Data Authorisations (OCDA).

Basildon Council is a member of the National Anti-Fraud Network and so has access to the Single Point of Contact. Applicants within the Council are required to consult a NAFN SpoC throughout the authorisation process, including before referring the case to a designated person within the authority for approval. The SpoC will provide advice to applicants and designated persons, ensuring that the local authority acts in an informed and lawful manner.

6.6 Authorisation Forms

6.6.1 Prior to obtaining judicial approval for an authorisation or renewal, all surveillance should be authorised by a prescribed person as prescribed for the purposes under Section 30 of RIPA and The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003, using the appropriate forms, which are: -

6.6.2 **Application** for authority for directed surveillance; which requests specific information enabling the Authorising Officer to consider the request. The proposals should be compatible with the objectives of the surveillance. A written authorisation granted by an authorising officer will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the day when the authorisation was granted by the JP. When completing an application for a warrant or authorisation, the public authority must ensure that the case for the warrant or authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation.

6.6.3 **Review – ** in each case, Authorising Officers must consider the need for a review at the appropriate time according to the nature of the objective of the surveillance and both the Authorising Officer and the Investigating Officer should enter this into an appropriate diary or calendar system. It is good practice for Authorising Officers in any event to review authorisations on a monthly basis unless they consider they should take place more or less frequently (if so, it is suggested that the reasons should be recorded). More frequent reviews may be required where the activity involves a high level of intrusion into private life, or significant collateral intrusion, or where particularly sensitive information might be obtained.

6.6.4 Reviews for Directed Surveillance must record:
- Any significant changes to the information in the previous authorisation;
- Why it is necessary to continue with the surveillance;
- The content and value to the investigation or operation of the information so far obtained by the surveillance; and
- An estimate of the length of time the surveillance will continue to be necessary
- The results of any review should be retained for at least three years but best practice does indicate that it would be desirable for these records to be kept for five years. Therefore, the Council will keep these reviews for five years.

6.6.5 During a review, the reviewing officer may cancel aspects of the authorisation or warrant, for example to cease directed surveillance against one of a number of named subjects or to discontinue the use of a particular tactic.

6.6.6 **Renewal** of directed surveillance authorisation; for use when it is considered necessary for the authorisation to continue. A renewal should be sought and a renewal form completed to facilitate this. It is vital that, if a renewal is required, the completed form is submitted to an Authorising Officer in sufficient time to allow it to be considered and to be approved by a Justice of the Peace **prior** to the expiry of the existing authorisation.

6.6.7 **Cancellation** of directed surveillance authorisation; for use when the directed surveillance no longer meets the criteria for authorisation. The cancellation form will normally be authorised by the officer who last renewed or authorised the surveillance and must be completed as soon as the requirement for surveillance ceases. Even if an authorisation has reached its time limit and has ceased to have effect, it does not lapse and must still be formally cancelled. The responsibility to ensure authorisations are cancelled rests primarily with the officer in charge of the investigation who should submit the request for cancellation. However, if the Authorising Officer who authorised the directed surveillance is satisfied it no longer meets the criteria upon which it was authorised, he must cancel it and record that fact in writing, even in the absence of any request for cancellation.

6.6.8 **Refusal –** whilst there is no form for refusal, the Authorising Officer should notify Legal Services and provide copy documentation when an application has been made but has been refused by either an Authorising Officer or a Justice of the Peace
Examples of each form are annexed to this Policy for information only. In order to ensure that current forms are used, these should be obtained from the Gov.uk website.

The specific situations not requiring authorisation are detailed at paragraph 2.30 of the 2014 Covert Surveillance and Property Interference Revised Code of Practice.

6.7 Collateral Intrusion

6.7.1 If at any stage during the surveillance it becomes apparent that there is unexpected interference into the privacy of persons who are not the original subject of the investigation (this is called collateral intrusion) then this information and any other matters that arise of a similar sensitive nature, should be brought to the Authorising Officer's attention. This will enable the Authorising Officer to reconsider the original authorisation taking into consideration the new information. The Authorising Officer should particularly bear in mind the proportionality of the surveillance in this situation. Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved.

6.7.2 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance or property interference activity.

Collaborative Working

6.8.3 Section 4.32 of the Code of Practice (Covert Surveillance and Property Interference) confirms that in some circumstances it may be appropriate or necessary for a public

authority to work with third parties who are not themselves a public authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of a public authority, then they are acting as an agent of that authority and any activities that third party conducts which meet the 2000 Act definitions of directed or intrusive surveillance or amount to property interference for the purposes of the 1994 or 1997 Act, should be considered for authorisation under those Acts by the public authority on whose behalf that activity is being undertaken. Similarly, a surveillance authorisation should also be considered where the public authority is aware that a third party (that is not a public authority) is independently conducting surveillance and the public authority intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation being undertaken by that public authority.

6.8.4 Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance or property interference is taking place, and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance or property interference. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise, they should consult a senior officer within the police force area in which the investigation or operation is to take place. Moreover, public authorities should seek to avoid duplication of authorisations as part of a single investigation or operation where possible.

6.9 Central Records

6.9.1 Each Authority should maintain a central record (register) relating to all authorisations, giving details of what the authorisation was for and the dates during which surveillance has been carried out. The Council's central record is kept by Legal Services for a period of at least 5 years, as is indicated in best practice.

6.10 Emergency Situations

6.10.1 If an officer finds themselves in an urgent situation which requires directed surveillance to be undertaken then an authorisation for the directed surveillance must be granted by an authorising officer. Approval will then need to be obtained from a Justice of the Peace.

6.10.2 In most emergency situations where the Police have the power to act, then the Police are able to authorise activity under RIPA without prior judicial approval. A RIPA authority is not required in immediate response to events or situations where it is not reasonably practicable to obtain it. The monitoring of social media accounts would not in general be considered appropriate in an emergency situation (Section 3.32).

6.10.3 It will not be urgent where the need for authorisation has been neglected or is of the Officer's own making. These rules must not be used where there has been a failure to obtain authority at the appropriate time.

7. Covert Human Intelligence Source (CHIS)

7.1.1 **A person is a covert human intelligence source if:-**

(a) He establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

(b) He covertly uses such a relationship to obtain or to provide access to any information to another person; or

(c) He covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

(d) The relationship is used covertly if and only if it is conducted in a manner calculated to ensure that one party is unaware of its purpose.

7.1.2 This does not apply to circumstances where members of the public volunteer information to the Council. However, someone may inadvertently become a CHIS as a result of covertly supplying information to the Council if he is obtaining this information in the course of or as a result of the existence of a personal or other relationship. A specific issue arises as to whether someone becomes a CHIS because the Council issues them with diary/monitoring sheets and asks them to tell them of any further problems (i.e. anti-social behaviour cases).

This does not require specific authorisation unless a personal relationship between the alleged perpetrator and the complainant/witness exists or is cultivated (see below). Any authorisation must be sought on the CHIS application, and the officers able to give authorisation are the same as those designated as Authorising Officers for covert surveillance. It is important to establish whether someone is a CHIS as a duty of care would be owed to such a person who may be at risk of reprisals if the information is acted on.

7.2 Authorisations

7.2.1 These work in a similar way to directed surveillance and must be authorised in writing and require authorisation from the authorising officer. The Council must obtain an order approving the grant or renewal of an authorisation from a Justice of the Peace before it can take effect. The use of vulnerable sources should only take place in exceptional circumstances. Juveniles can never be used as sources against their own parents but can be used subject to special safeguards (see 7.9 below).

7.2.2 ***Information to be given in applications for authorisation: -***

- Details of the purpose for which the source will be deployed.
- The grounds on which authorisation is sought (i.e. detection of crime).
- Where a specific investigation is involved details of that investigation.
- Details of what the source will be tasked to do.
- Details of the level of authority required.
- Details of potential collateral intrusion.
- Details of any confidential material that might be obtained as a consequence of the authorisation.

7.2.3 It is important that the Council considers an authorisation whenever the use and conduct of a CHIS is likely to engage an individual's rights under Article 8, whether this is through obtaining information, particularly private information, or simply through the covert manipulation of a relationship. An authorisation will be required if a relationship exists

between the subject and the CHIS, even if specific information has not been sought by the Council.

7.2.4 When a relevant source is deployed to establish their “legend”/build up their cover profile, an authorisation must be sought under the 2000 Act if the activity will interfere with an individual’s Article 8 rights. The individual does not have to be the subject of a future investigation. Interference with any individual’s Article 8 rights requires authorisation under the 2000 Act.

7.3 Online Covert Activity

7.3.1 The use of the internet may be required to gather information prior to and/or during a CHIS operation, which may amount to directed surveillance. Alternatively, the CHIS may need to communicate online, for example this may involve contacting individuals using social media websites. Whenever the Council intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. The council must recognise that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites. Any activity likely to interfere with an individual’s Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that information is likely to be obtained, an authorisation (combined or separate) must be sought.

7.9 Juvenile CHIS

7.9.1 Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. As a matter of policy, the Council does not engage in the use of Juvenile Covert Human Intelligence Sources.

7.10 Central Records

Record Keeping

7.10.1 The Council must keep a central record of all authorisations granted for the use of CHIS. The central record is maintained by Legal Services. The record need only contain the name, code name, or unique identifying reference of the CHIS, the date the authorisation was granted, renewed or cancelled, and an indication as to whether the activities were authorised by an Officer directly involved in the operation.

Errors

7.10.2 Wherever possible, any technical systems should incorporate functionality to minimise errors. A person holding a senior position within each public authority (which in this context is considered to be the Senior Responsible Officer with the support of Legal Services), must undertake a regular review of errors and a written record must be made of each review. This will be subject to consideration as part of the work of the RIPA Working Group. An error must be reported if it is a “relevant error”. Under section 231(9) of the 2016 Act, a relevant error for the purpose of activity covered by this code 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 Judicial Commissioner. Errors should be reported to the Commissioner within ten working days. Further guidance and additional

detail for detecting and handling errors is available in section 8.6 to 8.18 of the Revised Code of Practice for Covert Surveillance.

8. The Role of Elected Members

8.1 Elected members of local authorities have a role to play in the review of the use of directed surveillance and CHIS. However, the Codes are clear that elected members should not be involved in making decisions in relation to specific authorisations.
Paragraph 3.35 of the revised Code of Conduct for Covert Surveillance, and paragraph 3.27 of the revised Code of Conduct for CHIS, state that members of a local authority should review the authority's use of RIPA and set the corporate policy at least annually, and should consider internal reports on the use of RIPA on a quarterly basis to ensure that it is being used consistently and within the scope of this policy, and that the policy remains fit for purpose. An annual report (during each municipal year) will be submitted to the Audit and Risk Committee describing the Council's use of RIPA powers over the previous year and highlighting any proposed amendments to this policy and seek approval of those changes.

Council Promises

Use the table below to provide a visual display of how this Policy will impact on the delivery of the five corporate promises. You may wish to expand on each point, as required.

	Levels of Impact			
Corporate Promises	High	Medium	Low	None
1.A place where people are happy, healthy and active		X		
2.An attractive and welcoming place that people are proud to call home			X	
3. A place that encourages businesses to grow and residents to succeed			X	

9. Outcomes and Priorities

9.1 The high level strategic goal and priority of the Policy are set out below.
Outcome – To effectively use RIPA powers to undertake a range of enforcement functions to keep the public safe and bring criminals to justice, whilst protecting individuals' rights to privacy.
Priority – To secure compliance with the legislative provisions that govern the use of covert surveillance and the management of covert human intelligence sources.
These will relate to specific areas within each outcome.

10, Links to other Corporate Policies or Partner documents

10.1 Regulatory Services Enforcement Policy
Service specific enforcement policies
CCTV Surveillance Policy

11. Appendices (including Procedures)

APPENDIX 1

Glossary of Terms

Private Information - in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. The definition of private information has been given a wide interpretation by the Courts and will include business information in appropriate circumstances. Where private information is gained as a result of covert surveillance in circumstances where a person would have a reasonable expectation of privacy then a directed surveillance authorisation may be considered appropriate.

Non-private Information - may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects (such as the class to which a cargo ship belongs for example).

Confidential information - includes, though is not limited to confidential personal information, confidential constituent information and journalistic material.

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified by it. Such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

Confidential constituent information is information relation to communications between a Member of Parliament and a constituent in respect of constituency matters.

Confidential journalistic material includes material acquired or created for the purpose of journalism and held subject to an undertaking to hold it in confidence as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

Legally Privileged Information – Matters subject to legal privilege are defined in s98 of the 1997 Act. This includes certain communications between professional legal advisers and their clients or persons representing the client.

APPENDIX 2

Directed Surveillance Procedure

Role of Authorising Officers

Authorising Officers do not only cover investigations carried out within their own services - any Authorising Officer may give authorisation in relation to surveillance to be carried out by officers from a different service.

Paragraph 5.7 of the amended Code of Practice for Covert Surveillance recommends that Authorising Officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that there are occasions where this may be unavoidable, for instance in cases of urgency. If an operation is authorised by an Authorising Officer who is involved, this should be highlighted within the central register, and the attention of the Commissioner drawn to the authorisation at the next inspection.

Any officer authorising such decisions must ensure that he or she is properly trained so that the decision is made in accordance with the law. It is important that the person seeking authorisation and the Authorising Officer ensures that the decision to take (and it is recommended not to take) action is properly documented with full reasons. Guidance is available on the Legal Services Home Page intranet under “Service Documents” - “RIPA” - “Application form with prompting questions”, together with course notes. If in doubt, please speak to a member of Legal Services. Comments should be put in the Authorising Officer’s Statement box in the application form and not just “I agree”. Authorising Officers must consider carefully any factors identified and set out in paragraph 5.8 below and record their reasons.

It is also important to note that the Authorising Officer’s job does not stop should s/he agree to authorisation. That person must keep the investigation under review, particularly if information may be obtained about someone other than the target of the surveillance (collateral intrusion). Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes.

The authorising officer or person considering issuing the warrant should ensure appropriate safeguards for the handling, retention or destruction of such material in accordance with chapter 9 of the CHIS code, as well as compliance with data protection requirements.

In all surveillance the risks should also be assessed properly and kept under review. So that there is a proper review system, officers should record the date when the authorisation should be reviewed. Whilst this can be the full 3 months (less a day) permitted the review will invariably be a much shorter period.

The Service Director acts as the Council’s ‘Senior Responsible Officer’ ensuring that all authorising officers are of an appropriate standard. (NOTE: See also paragraph 7 of this policy for the role of the Senior Responsible Officer.)

What the Authorising Officer must take into account

Upon turning their mind as to whether or not authorisation is warranted in a particular circumstance the Authorising Officer has to be satisfied on a two-stage test of necessity and proportionality. Necessary in this context means that nothing else will do, and it presupposes that the Investigating Officer has considered other options.

Under s28(3) of the 2000 Act an authorisation for directed surveillance may be granted if the senior authorising officer believes that:

- It is in the interests of national security.
- it is for the purposes of preventing, or detecting crime or preventing disorder
- It is in the interests of national security
- It is in the interests of the economic well-being of the UK
- It is in the interests of public safety
- It is for the purpose of protecting public health.
- It is for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department or
- For any other purpose described by an order made by the Secretary of State.

In considering whether or not the proposed surveillance is proportionate, the Authorising Officer will need to consider whether there are other more non-intrusive ways of achieving the desired outcome; the least intrusive means should always be chosen. The Authorising Officer ought also to pay attention to the means by which the surveillance is proposed and whether or not that means it is the most appropriate for the particular circumstances of the case. Does it, for example, minimise collateral intrusion (invasion of third parties' privacy) and is it readily workable?

The Authorising Officer must take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance and measures must be taken whenever practicable to avoid or minimise the intrusion.

The Court will consider the least intrusive method proportionate. This involves a balancing exercise of the activity on the subject and others who may be affected by it against the need in operational terms.

The activity will not be proportionate if it is excessive in the circumstances – each case will be judged and be unique on its merits. Authorising Officers should be keen to limit the scope of the authorisation where at all possible and where such limitation is imposed the Authorising Officer must bring such limitation to the attention of the Investigating Officer.

Even in cases of serious crime or disorder, it may be possible to obtain the necessary evidence by means other than covert surveillance, and the least intrusive method of investigation should still be considered in the first instance. Special care needs to be given in relation to joint operations with other agencies and where the Council employs an agent to carry out investigations on its behalf.

Record Keeping

Each Department must send a copy of any authorisation to Legal Services and keep it updated as to renewals, cancellations etc. It is also recommended that refusals of authorisations are sent to Legal Services.

To assist Legal Services in maintaining the central record, and to make it easier to trace authorisation forms in the event of an inspection or query, individual departments should

not enter their own reference number on authorisation forms. A unique reference number will be assigned to each authorisation form upon its receipt by Legal Services, prior to it being placed in the central record, and the investigating officer notified of that number. A full list of the matters to be recorded can be found in paragraphs 8.1 – 8.3 of the revised Code of Conduct for Covert Surveillance. See Appendix 4 for a blank copy of the Central Record, to see the information required.

RIPA records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal, established under Part IV of the Act, to carry out its functions. The Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates, particularly where continuing conduct is alleged.

Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for these purposes includes an organisation, an association, or combination of persons (see section 81(1) of RIPA), as well as an individual.

Although records are only required to be retained for at least three years it is desirable if possible to retain the records for five years and the Council will keep these records for five years.

Covert Human Intelligence Sources Procedure

6.3 What the Authorising Officer must take into account
Under s29(3) of the 2000 Act an authorisation for the use or conduct of a CHIS may be granted by an authorising officer where they believe that:

1. The authorisation is necessary and
- In the interests of national security.
- For the purposes of preventing and detecting crime or of preventing disorder.
- In the interest of the economic wellbeing of the UK.
- In the interests of public safety
- For the purpose of protecting public health
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or for any other purpose prescribed in an order made by the Secretary of State.

2. It is proportionate to what it seeks to achieve & appropriate arrangements for managing the source,

3. It should take into account the risk of collateral intrusion,

4. It ensures that particular care is taken concerning confidential material,

5. Any adverse impact upon the community confidence has been considered,

6. Any risk to the source has been appropriately assessed.

Sometimes authorisation is needed in the process of cultivating the source where this would infringe the privacy of the source. The cultivation process itself may require authorisation if it involves directed surveillance, for example.

Record Keeping

As with authorisations for directed surveillance, the central register is kept and maintained by Legal Services (Solicitor to the Council) to whom every authorisation should be sent.

Detailed records of the authorisation must also be kept by the department carrying out the activities. A full list of the matters to be recorded can be found at paragraphs 7.4, 7.5 and 7.6 of the 2018 revised Code of Conduct for CHIS. Those records should be kept for at least five years. This must be done in such a way as to preserve the confidentiality of the source.

The revised Code of Practice for CHIS suggests that a record should also be maintained for human sources who do not fall within the definition of a CHIS. This will assist the Council in monitoring the status of human sources, and to determine if and when that source becomes a CHIS.

The 2014 revised Code of Practice for CHIS confirms that the Investigatory Powers Tribunal will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so may consider complaints made more than one year after the conduct to which the complaint relates. This is particularly true where continuing conduct is alleged. It is therefore suggested at paragraph 7.3 of the revised 2014 Code of Conduct for CHIS that it is desirable to keep records for at least five years and the Council will do so.

Duration of authorisation

A written authorisation (except a juvenile source which is only valid for 4 months) unless renewed will cease to have effect at the end of a period of 12 months beginning with the day on which it took effect.

Reviews & Renewals

A review should be carried out and the Authorising Officer satisfied that the conditions for authorisation continue to be met before the authorisation is renewed for a further period. Approval for the renewal must then be sought from a Justice of the Peace. Provided conditions continue to be met authorisation can be renewed more than once. The renewal extends the time from when the authorisation would expire (but for the renewal) so the renewal decision should be taken shortly before expiry of the authorisation. Renewals can be granted for a further period of 12 months only. The results of the Review should be kept for at least three years and it is desirable best practice for them to be kept for five years. The Council will therefore keep the results of Reviews for five years.

It is necessary that the Council record:

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

- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- whether any privileged material or information was obtained as a result of activity undertaken under the authorisation, to which the safeguards in chapter 9 of this code should apply;
- the results of regular reviews of the investigation or operation.

Cancellations

Authorisations should be cancelled where the conditions justifying authorisation are no longer satisfied. The authorising officer should do this in writing although it is suggested that the officer seeking authorisation should also seek cancellation where s/he becomes aware that the conditions are no longer satisfied. There is a standard form for recording this. Although some authorisations will be renewed on a number of occasions, every authorisation must be cancelled at the end of the surveillance operation.

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) as soon as reasonably practicable. The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation. However it is good practice that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

APPENDIX 3

Documents

(For information only – the forms are available from gov.uk website)

1. PROCEDURE FOR AN APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE.

2. DIRECTED SURVEILLANCE - APPLICATION FORM

3. JP (AUTHORISATION FORM)

4. DIRECTED SURVEILLANCE - RENEWAL FORM

5. DIRECTED SURVEILLANCE - REVIEW FORM

6. DIRECTED SURVEILLANCE - CANCELLATION FORM

7. BLANK COPY OF CENTRAL RECORD

8. CHIS – APPLICATION FORM

9. CHIS – RENEWAL FORM

10. CHIS – REVIEW FORM

11. CHIS – CANCELLATION FORM

APPENDIX 4

PROCEDURE FOR AN APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

1. Ensure the application form has been approved by the Authorising Officer

2. Contact the Admin Team at Essex Magistrates Court as soon as possible to arrange a hearing.

3. Provide the Justice of the Peace (JP) with a copy of the original RIPA authorisation or notice and the supporting documents which set out the case.

4. The original authorisation or notice should be shown to the JP

5. Provide the JP with a partially completed judicial application/order form.

6. The order form will be completed by the JP and this will need to be retained by the local authority.

7. When out of hours access to a JP is required – need to look at local arrangements (not to be used where a renewal has not been processed in time). In most emergency situations where the police have the power to act they can authorise activity under RIPA without prior JP approval. No authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it i.e. during routine inspections.

8. At the hearing – officers to be formally designated to appear (check authorisations), be sworn in and present evidence or provide information as required by the JP.

9. Hearing is in private and the JP will consider the RIPA authorisation or notice and the judicial application/order form. The JP may have questions to clarify points or require additional reassurance on matters.

10. Officers attending court may be asked questions on the policy and practice of conducting covert operations together with detail of the case itself.

11. JP to make decision that at the time of granting or renewal there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate.

12. The forms and supporting information must themselves make the case. If more information is required to determine whether the application or notice has met the tests then the JP will refuse the authorisation.

13. Outcomes; approval the grant or renewal of an authorisation or notice, refuse to approve the grant or renewal of an authorisation or notice (if this is the case then we will need to consider the reasons for the refusal), refuse to approve the grant or renewal and quash the authorisation or notice – if the JP is considering quashing this then we have 2 business days from the date of the refusal in which to make representations.