COMPLIANCE WITH THE REGULATION OF INVESTIGATORY POWERS

Basildon Council
BASILDON • BILLERICAY • WICKFORD

Key Information

Author:	Phil Easteal, Group Manager (Regulation)
Section/Directorate:	Regulatory Services
Service Impact Assessment:	17 September 2015
External Consultation:	The nature of the policy and the fact that it does not impact on any one particular interest group or sector of the community means that public consultation is impractical.
Internal Consultation:	Internal consultation has been undertaken with representatives of relevant services to inform the development of this Policy. Specifically, application of the policy and maintaining its accuracy and relevance is kept under regular review by the Council's RIPA Working Group.
Background Information:	The necessity for this policy arises from the Regulation of Investigatory Powers Act 2000, as amended, together with associated Orders and Codes of Practice.
Policy Approval – Officer Level	The appointed RIPA 'Senior Responsible Officer' is the Service Director who also chairs the RIPA officer working group and keeps these arrangements under review
Policy Approval – Member Level	Audit and Risk Committee
Policy Review Date:	March 2023
Service Impact Assessment Review Date:	March 2023

Content

1. Introduction

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 of a covert nature.

In conducting these 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 2014 Covert Surveillance Code and the Covert Human Intelligence Service Code of Practice.

In 2010, parliament passed a revised Order and an amended Order was passed in 2012. Amended Codes of Practice for Covert Surveillance and Property Interference and for Covert Human Intelligence Sources were issued in 2014. Reference to these revised documents is made throughout this Policy. If in doubt, reference should be made to the Codes of Practice, which can be obtained from Legal Services.

The revised Codes of Practice contain examples to illustrate situations when authorisation might or might not be required. Whilst these examples may be useful as a starting point in considering whether authorisation is required, they should not be relied upon and are not a substitute for proper, detailed consideration of the individual circumstances of each proposed operation.

The revised Codes of Practice that came into force on 10 December 2014 confirm that In England and Wales local authorities can only authorise directed surveillance under RIPA to investigate offences which attract sentences of **six months** or more or relate to the **underage** sale of alcohol or tobacco.

In conclusion, this Act has far reaching implications for many areas of work carried out by the Council. The Act does not in any way restrict its operation to specific functions and therefore it is imperative that any officer who might be carrying out surveillance, and authorising officers, are fully aware of when the need arises for an authorisation to be obtained. This document only sets out the brief principles involved and it must be stressed that any officer requesting authorisation and particularly those persons empowered by the Council to grant authorisations must ensure that they receive full and proper training before dealing with any authorisations.

However, a considerable amount of what the Council does is OVERT so that the person being investigated is fully aware of the situation. This will never need authorisation.

As of 1 November 2012 once an authorisation for directed surveillance or a CHIS has been granted, approval will need to be obtained from a Justice of the Peace. 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.

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.

2. Executive Summary

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.

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).

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

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).

3. Policy Statement / Vision

The Council wants to ensure that there is organisational understanding of the powers set out in RIPA and more importantly compliance with the provisions set out therein. It is essential to ensure that there is both understanding and compliance in order to ensure that the Council acts in a manner that is fully compliant with the statutory framework in which it operates. It is also essential so that the Council does not breach the Human Rights Act 1998 and that any evidence obtained as part of an investigation is admissible in Court where appropriate.

The Council hopes to achieve this vision by the adoption of this Policy, providing training to staff as required and continuing to keep the legislation and guidance under review.

4. Context

4.1 National – The key drivers of the Policy is to ensure that the Council is fully compliant with RIPA.

4.2 Local – The new updated Policy is needed to ensure that reference is made to any changes in the legislative framework in the new policy and that the new agreed authorised persons are 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 utilize the powers available to it in compliance with RIPA and how the Council will do so whilst promoting its promises.

4.3 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 in the Council's Corporate Plan 2017-2021 - Transforming Basildon

Corporate Promises	Levels of Impact			
	High	Medium	Low	None
Strong, safe and healthy communities with access to quality homes	X			
Vibrant town centres and a thriving economy for everyone			X	
Enhanced local environment and increased pride in our borough			X	

4.4 Consequences of Failure to Comply with the RIPA

Article 8 of the Human Rights Convention introduced a new concept in English Law, 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". Hence a legal framework to authorise surveillance was required and RIPA was introduced.

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. 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 case law indicates this is less likely to cause problems. This policy document recommends that authorisations are always obtained in accordance with the Act, where appropriate.

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.

4.5 Office of Surveillance Commissioners

RIPA provides for a Chief Surveillance Commissioner, whose remit it is to provide an independent oversight of the use of the powers contained within Part 2 of the Act, by public authorities.

The OSC undertakes periodic inspections. The aim of any inspection is to be as helpful as possible in providing feedback on best practice, recurring problem areas and remedies. The Council welcomes the findings of OSC inspections and has always taken the recommended steps to improve RIPA compliance.

5. Surveillance

There are two types of activity that may be relevant to investigations carried out in local government: **directed surveillance** and **covert human intelligence sources** ("CHIS").

This section covers directed surveillance. CHIS is covered in section 6.

Directed surveillance does not include entry on or interference with property or wireless telegraphy, nor does it include interception of communications sent by post or by telecommunication systems. These can only be carried out by the Secretary of State, Police or intelligence agencies (depending upon the situation). However, you should not rule out directed surveillance simply because you might overhear telephone conversations, but you cannot deliberately place a device so as to hear such conversations.

The definition of Surveillance includes:

- 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.

5.1 Definition of Directed Surveillance

Very often surveillance is conducted with the intention of that person being unaware that the surveillance is or may be taking place i.e. **covertly**. 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.

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 will be required.

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's private or family life**.

- is conducted in such a way as to obtain a detailed picture about the manner in which that person conducts their **private life, activities and associations**.

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.

5.2 Online Covert Activity

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 private information is likely to be obtained, 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.

5.3 Intrusive Surveillance

Is defined as covert surveillance that:

- is carried out in relation to anything taking place on any **residential premises or in private vehicle**; and

- involves the **presence** of an individual on the premises or in the vehicle or is carried out by means of a surveillance devise.

This 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 for signage etc.

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.

It must be remembered that local authorities cannot authorise intrusive surveillance.

5.4 Private, Confidential and Legally Privileged Information

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.

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 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.

5.5 Authorisation Forms

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: -

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. However, all authorisations must be cancelled eventually (some may be renewed a number of times but still must be cancelled eventually).

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). 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.

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.

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.

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 Home Office website or from the Legal Services (Litigation) intranet homepage.

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

5.6 Collateral Intrusion

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.

5.7 Authorising Officers – who can make a decision?

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 stipulates that only prescribed officers can sign authorisations and the level of these positions must be "Director, Head of Service, Service Manager or equivalent" (and more senior posts).

Historically there were a number of posts designated as Authorising Officers. However, following an inspection by the Office of Surveillance Commissioners, it was recommended that the number of Authorising Officers be reduced.

In accordance with that recommendation, by a Cabinet Member Decision Record dated 16th April 2009, the Constitution was amended 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 Service Director, Service Manager Revenues and Business Support, Revenues and Benefits Operational Manager, Environmental Health Manager and the Group Manager (Regulation).

AND

b) The Managing Director (or a Chief Officer in his absence) only may authorise Juvenile Covert Human Intelligence Source applications.

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.

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). 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.)

5.8 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.

The Serious Crime Test

As of 1 November 2012, 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.

As of 1 November 2012, 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. The issues below must be considered.

- Ensure compliance with the data protection requirements and any other relevant codes of practice and 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 above).
- Judge 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 by relation to the gravity of the mischief being investigated.

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.

5.9 Central Records

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. Since 1ST January 2003 the Council's central record has been kept by the Solicitor to the Council for a period of at least 3 years from the ending of each authorisation. It is best practice to keep these records for five years. Therefore, the Council will keep these records for five years.

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. 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.

5.10 Emergency Situations

If you find yourself in an urgent situation which requires you to undertake directed surveillance then an authorisation for the directed surveillance must be granted by an authorising officer. You will then need to obtain approval from a Justice of the Peace.

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.

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.

6. Covert Human Intelligence Source (CHIS)

6.1 Introduction

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 can be sought on the same form as for directed surveillance, 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.

6.2 Definition of a CHIS

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.

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 interests of national security,*
    - *In the interest of the economic well being 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. Should take into account the risk of collateral intrusion,
4. Ensure particular care is taken concerning confidential material,
5. Any adverse impact upon the community confidence,
6. Assess any risk to the source.

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.

6.4 Authorisations

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 5.9 below).

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.

It is important that the Council considers an authorisation whenever the use if 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.

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.

6.5 Duration of authorisation

A written authorisation (except a juvenile source) 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.

6.6 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 the time 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.

6.7 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.

6.8 Online Covert Activity

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. 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 private information is likely to be obtained, an authorisation (combined or separate) must be sought.

6.9 *Juvenile CHIS*

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.

6.10 Record keeping

The Council must keep a central record of all authorisations granted for the use of CHIS. The central 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.

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 revised Code of Conduct for CHIS. Those records should be kept for at least five years 5 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.

7. Responsible Officer

A new recommendation of best practice under the revised Code of Conduct both for Covert Surveillance is that every public authority should have a Senior Responsible Officer who 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.

- Ensuring that Authorising Officers are of an appropriate standard.

The Senior Responsible Officer should be a member of the corporate leadership team, and should have the status of an Authorising Officer. Within Basildon Council, the Senior Responsible Officer is the Service Director. The Senior Responsible Officer will be informed by the RIPA Working Group and by the Solicitor to the Council.

8. The Role of Elected Members

An additional requirement arising from the latest RIPA rules is that for elected members of local authorities to be involved in the review of the use of directed surveillance and CHIS. However, the revised 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.

Furthermore, an annual report 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.

9. Outcomes and Priorities

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

Refer to service enforcement policies, for example the Regulatory Services Enforcement Policy, and policies and procedures relating to operation of CCTV.

11. Appendices

See following list of available documents.

APPENDIX OF DOCUMENTS

(For information only)
Refer to electronic versions of templates where not provided here.

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. APPLICATION FORM

3. JP (AUTHORISATION FORM)
4. RENEWAL FORM
5. REVIEW FORM
6 CANCELLATION FORM
7. BLANK COPY OF CENTRAL RECORD

APPENDIX 1

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.

Monday to Friday
10am to 5pm

BasildonCouncil
BASILDON · BILLERICAY · WICKFORD

For translations, Large Print and Braille please call

Para obtener traducciones, por favor llame al número (Spanish)
অনুবাদের জন্য দয়া করে ফোন করুন (Bengali)
Aby uzyskać pisemne tlumaczenie proszę dzwonić pod numer (Polish)
如需翻译，请拨打 (Mandarin)
O překlad prosím zavolejte (Czech)
若需翻譯，請致電 (Cantonese)
Чтобы получить перевод на русский язык, позвоните по телефону (Russian)
Tercüme için lütfen arayın (Turkish)
برای ترجمه با این شماره تماس بگیرید (Farsi)
Pour obtenir une traduction, composez le (French)
بۆ تەرجومە تەلەفۆن بکە بۆ ژمارەی(Kurdish)
للترجمة يرجى الاتصال (Arabic)
Per perkthim me shkrim ju lutem merni ne telefon (Albanian)
ભાષાંતર માટે કૃપા કરીને ફોન કરો (Gujarati)
ट्रांस्लेशन के लिये कृपया कॉल करें: (Hindi)
Pentru traducere va rugam sunati (Romanian)
Untuk terjemahan harap hubungi (Indonesian)
Kwa tafsiri, tafadhali piga simu (Kiswahili)
ਅਨੁਵਾਦ ਵਾਸਤੇ ਕਿਰਪਾ ਕਰਕੇ ਕਾਲ ਕਰੋ (Punjabi)
Kana muchida kuturikirwa, tapota ridzai runhare kuna (Shona)
Pre preklad prosim volajte (Slovak)
Nếu quí vị cần dịch tài liệu, xin vui lòng gọi theo số (Vietnamese)

01268294791

Language Line services

Customers with a hearing or speech impairment can contact us using the Text Relay service. Dial 18001 followed by the full telephone number of the service you require. Calls are charged at your telecommunications provider's standard rate.