South Cambridgeshire District Council

Regulation of Investigatory Powers Act 2000
Corporate Policy & Procedures

Statement of Intent: South Cambridgeshire District Council attaches a high value to the privacy of citizens. It will adhere to the letter and to the spirit of the Act and will comply with this policy.

Contents

1 Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that privacy is only interfered with where the law permits and where there is a clear public interest justification.

1.2 The purpose of this policy is to explain the scope of RIPA and the circumstances where it applies to the Council. It provides guidance on the authorisation procedures to be followed in the event that surveillance is needed. This policy sets out the correct management of the process by the Council.

1.3 This policy also ensures that activities that should be subject to RIPA authorisation is recognised as such and that appropriate authorisation is sought. It also seeks to ensure that any activity which should be carefully monitored, but which is not subject to RIPA authorisation, is still given correct authority and scrutiny.

1.4 The Protection of Freedoms Act 2012 imposed new restrictions on the circumstances in which the Council is permitted to use directed surveillance and this policy has been updated to take into account these new restrictions. Separate guidance has been issued by the Home Office which specifies the procedure for the consideration and approval of applications by Magistrates and this policy must be read in conjunction with that procedure and documents issued by the Office of the Surveillance Commissioner.

1.5 The Executive Director (Corporate Services) is the Senior Responsible Officer for the RIPA process for the Council. All staff involved in the process must take their responsibilities seriously in order to assist with the integrity of the Council's processes and procedures.

1.6 In preparing this policy the Council has followed the Revised Codes of Practice (April 2010) produced by the Home Office and considered guidance provided by the Office of Surveillance Commissioners.

1.7 In the case of any uncertainty advice should be sought from an Authorising Officer or the Head of Legal Practice, who is the Council's RIPA Monitoring Officer.

1.8 Copies of the Codes of Practice can be found on the Council's RIPA Intranet page and at the following links:

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

1.9 Further guidance can also be obtained from the Office of Surveillance Commissioners website:

https://osc.independent.gov.uk/

2 Background

2.1 The Human Rights Act 1998 brought into UK law many of the provisions of the 1950 European Convention on Human Rights and Fundamental Freedoms. Article 8 requires the Council to have respect for people's private and family lives, their homes, and their correspondence. These subjects can be referred to as "Article 8 rights".

2.2 The Human Rights Act makes it unlawful for any local authority to act in a way which is incompatible with the European Convention on Human Rights. However these are not absolute rights and are qualified by the ability of the Council to interfere with a person's Article 8 rights if :-

- such interference is in accordance with the law
- is **necessary**; and
- is **proportionate**

2.3 "*In accordance with the law*" means that any such interference is undertaken in accordance with the mechanism set down by RIPA and the Home Office Covert Surveillance Codes of Practice. The Codes of Practice deal with the use of Covert Surveillance and the use of persons such as informants and undercover officers who gather information in a covert capacity, known as a **Covert Human Intelligence Source or "CHIS**". Any covert activity must also meet the test of necessity and proportionality and these are dealt with later in this policy.

2.4 A considerable amount of observations are carried out in an overt capacity by Council employees carrying out their normal functions. These activities are general and routine and do not involve the systematic surveillance of an individual. RIPA is not designed to prevent these activities or regulate them.

2.5 RIPA also applies to the **Accessing of Communications Data** under Part 1, Chapter 2 of the legislation. The Council has produced separate guidance dealing with the accessing of communications data under the Single Point of Contact ("SPOC") provisions.

2.6 The Council has numerous statutory duties and powers to investigate the activities of private individuals and organisations within its jurisdiction for the benefit and protection of the greater public. Some of these investigations may require surveillance or the use of a CHIS. These may include:

- environmental health
- housing
- planning
- audit
- revenues and benefits fraud

2.7 RIPA provides a framework to control and supervise covert activities such as surveillance and the use of a CHIS in these criminal investigations. It aims to balance the need to protect the privacy of individuals against the need to protect others by the Council in compliance with its enforcement functions. Covert Surveillance and CHIS are covered by separate Codes of Practice which can be found on the Council's Intranet RIPA page.

3 When RIPA applies

3.1 RIPA applies to Public Authorities such as Local Authorities and permits them to conduct covert surveillance activities and use Covert Human Intelligence Sources (CHIS) such as informants and undercover officers only when the following two conditions are both met and when properly authorised by an authorising officer and a Magistrate:

For the "…***preventing or detecting conduct which constitutes one or more criminal offences or is or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences*****"**

and

"*an offence which is punishable, whether on summary conviction or on indictment by a maximum term of at least 6 months of imprisonment or certain other specified offences*"

3.2 It should be noted that the provision relating to the prevention of disorder is no longer included.

3.3 Using the RIPA application process helps protect the Council from legal challenges and provides the lawful authority for officers to conduct covert surveillance and use CHIS in connection with the prevention and detection of crime or of preventing disorder. South Cambridgeshire District Council and its staff have a responsibility to adhere to the legislation and the Human Rights Act. Any contract staff employed by South Cambridgeshire District Council to undertake such activity are also covered by the codes.

3.4 The RIPA Codes of Practice state where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

3.5 Public authorities are therefore strongly recommended to seek an authorisation under RIPA where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

3.6 In some instances it is not possible to obtain RIPA authorisation for surveillance activities due to the limited grounds set in the legislation where authorisation can be granted. It may be, however, that covert surveillance is still necessary and proportionate. This is dealt with later in this Policy but, as per s.80 of RIPA and para 355 of the explanatory notes "… *nothing in [the] Act makes any actions unlawful unless that is explicitly stated. The availability of an authorisation or a warrant does not mean that it is unlawful not to seek or obtain one. In this respect, the Act must be read with section 6 of the Human Rights Act, which makes it unlawful to act in a way which is incompatible with a Convention right*."

4 Surveillance Definitions

4.1 Surveillance

4.1.1 Surveillance is defined in paragraph 1.9 of the Revised Codes of Practice as:

"Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained."

4.2 Covert Surveillance

4.2.1 Covert Surveillance is defined in paragraph 1.10 of the Revised Codes of Practice as:

"Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place."

4.2.2 If activities are open and not hidden from the persons subject to surveillance such as Officers conducting Council business openly, e.g. a market inspector walking through markets, the RIPA framework does not apply because that is overt surveillance. Equally, if the subject is told that surveillance will be taking place, the surveillance is overt. This would happen, for example, where a noise maker is informed that noise will be recorded if it continues. RIPA does not regulate overt surveillance.

4.2.3 RIPA regulates only two types of Covert Surveillance which are:

- Directed Surveillance
- Intrusive Surveillance

4.2.4 <u>However, where the purpose of a surveillance operation is to obtain private information about a person, his family or what he does, the authorisation procedures set out in this policy should be followed and the surveillance treated as being "directed</u>".

4.3 Directed surveillance

4.3.1 Surveillance is directed surveillance (paragraph 2.2. of the Revised Codes of Practice) if the following are all true:

it is covert, but not intrusive surveillance;

it is conducted for the purposes of a specific investigation or operation;

it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);

it is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.

4.3.2 The planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

4.3.3 It is important that all activity that may constitute surveillance is recognised as such and correctly authorised, either as directed surveillance or, in some instances, as surveillance outside of RIPA as governed by this policy. Anything involving the use of concealed cameras or anything involving keeping covert observation on premises or people should be considered as potentially amounting to directed surveillance. In the case of uncertainty advice should be sought from the Head of Legal Practice.

4.4 Private information

4.5 Private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

4.6 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis.

4.7 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be considered appropriate.

5 Risks of not having correct RIPA Authorisation

5.1 If Investigators undertake covert activity to which this legislation applies without the relevant authority being obtained and the case progressed to criminal proceedings the defence may challenge the validity of the way in which the evidence was obtained under Section 78 of the Police and Criminal Evidence Act 1984. Should the evidence then be disallowed by a court, the prosecution case may be lost with a financial cost to the Council.

5.2 The person who was the subject of surveillance may complain to the Ombudsman who may order the Council to pay compensation. The activity may also be challenged through the civil courts under the Human Rights Act 1998 for breach of privacy.

5.3 A properly obtained and implemented authorisation under RIPA will provide the Council with lawful authority to interfere with the rights of the individual. It is not simply enough that an authorisation for surveillance is obtained. It must be properly obtained, implemented, managed, reviewed and cancelled.

6 Surveillance Outside of RIPA

6.1 There may be a necessity for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation such as in cases of serious disciplinary investigations. The Council still must meet its obligations under the Human Rights Act and therefore any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance will mirror that of RIPA-authorised surveillance, except that the activity will not require approval from a Magistrate.

6.2 An application will be made using the normal RIPA application form but these forms will not make any reference to the Act.

6.3 The authorising officer will be required to give the application the same degree of consideration and copies of all forms will be passed to the RIPA Monitoring Officer, who will keep a record of all activity separately from the records of RIPA-authorised surveillance

7 Immediate Response to Events

7.1 There may be occasions when officers come across events unfolding which were not pre-planned which then require them to carry out some form of observation. This will not amount to Directed Surveillance. However, as the Council is no longer able to grant urgent oral authority to conduct surveillance the officer must be prepared to explain their decisions in court should it be necessary. Therefore they should document their decisions, what took place, what evidence or information was obtained.

8 Recording of Telephone Conversations

8.1 The recording of telephone conversations connected to criminal investigations outside of the Councils monitoring at work policy for its own equipment falls under RIPA and provides, where one party to the communication consents to the interception, it may be authorised in accordance with section 48(4) of the 2000 Act. In such cases, the interception is treated as directed surveillance.

8.2 There may be occasions where this is required such as a witness who has text or voicemail evidence on their mobile telephone and SCDC require to examine the phone.

9 Intrusive surveillance

9.1 South Cambridgeshire District Council has no authority in law to carry out Intrusive Surveillance or activity under the Police Act 1997.

9.2 Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

is carried out in relation to anything taking place on any residential premises or in any 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 device.

9.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

9.4 A risk assessment of the capability of equipment being used on residential premises and private vehicles should be carried out to ensure that it does not fall into Directed Surveillance.

9.5 Commercial premises and vehicles are excluded from the definition of intrusive surveillance. However they are dealt with under the heading of Property Interference contained within the Police Act 1997.

10 Covert Human Intelligence Source (CHIS)

10.1 Definition

10.1.1 A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Fraud Hotline. Members of the public acting in this way would not generally be regarded as sources.

10.1.2 Under section 26(8) of the 2000 Act a person is a 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 information 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.

10.1.3 By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

10.1.4 By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

10.1.5 **The use by South Cambridgeshire District Council of a CHIS is expected to be extremely rare and if contemplated advice should be sought from the Head of Legal Practice urgently. Only the Chief Executive should authorise the use of a juvenile CHIS**.

10.2 Conduct and Use of a Source

10.2.1 South Cambridgeshire District Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation. The Handler of the source will usually be of a rank or position below that of the Authorising Officer.

10.2.2 The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

10.2.3 The **conduct** of a source is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

10.2.4 The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfill whatever tasks are given to them or which is incidental to it. **Both the use and conduct require separate consideration before authorisation.**

10.2.5 When completing applications for the use of a CHIS this will include who the CHIS is, what they can do and for which purpose

10.2.6 When determining whether a CHIS authorisation is required consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

10.3 Management of Sources

10.3.1 Within the provisions there has to be;

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare (**Handler**)
(b) at all times there will be another person who will have general oversight of the use made of the source (**Controller**)
(c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

10.3.2 The **Handler** will have day to day responsibility for:

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

10.3.3 The **Controller** will be responsible for the general oversight of the use of the source.

10.4 Tasking

10.4.1 Tasking is the assignment given to the source by the Handler or Controller by, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

10.4.2 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

10.4.3 **Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice**.

10.5 Security and Welfare

10.5.1 The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and

welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

11 RIPA Application and Authorisation Process

11.1 Application, Review, Renewal and Cancellation Forms

11.1.1 No covert activity covered by RIPA should be undertaken at any time unless it has been authorised by an Authorised Officer and a Magistrate and the appropriate forms completed at the appropriate time.

11.1.2 All the relevant forms for authorisation through to cancellation must be in writing using the standard forms which are available on the Council's Intranet site but officers must ensure that the circumstances of each case are accurately recorded on the application form (see Application Process).

11.1.3 If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject the respective applications forms and procedures should be followed and both activities should be considered separately on their own merits.

11.1.4 An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

11.2 Applications

11.2.1 All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer and then the Magistrate to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case*. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge*.

11.2.2 All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However they should not be involved in the sanctioning of the authorisation. Completed application forms are to be initialled by Line Managers to show that the quality check has been completed.

11.2.3 Applications whether authorised or refused will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations. To obtain this number contact the Legal Services team.

11.2.4 The procedure for submitting applications to Magistrates for consideration is set out in the procedure issued by the Home Office for this purpose.

11.3 Duration of Applications

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Juvenile Sources	1 Month

Renewal	12 months

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire.

11.4 Reviews

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

11.4.2 In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

11.4.3 Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably a new application form may be more appropriate. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

11.4.4 Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

11.5 Renewal

11.5.1 If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of three months. Like applications, all renewals must also be considered by a Magistrate

11.5.2 A renewal takes effect on the day on which the authorisation would have ceased.

11.5.3 An application for renewal should not be made until shortly before the authorisation period is drawing to an end but the applicant must consider the need to allow sufficient time for consideration by the authorising officer and any potential delay in getting the matter before a Magistrate for consideration.

11.5.4 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity.

11.5.5 A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained.

11.5.6 The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

11.6 Cancellation

11.6.1 The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

11.6.2 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraphs 2.14 - 2.15 in the Codes of Practice).

11.6.3 **It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by Central Register**.

11.6.4 The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what, if any, images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc.

11.6.5 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

11.7 Authorising Officers

11.7.1 Officers who are designated "Authorising Officers" may authorise written applications for the use of directed surveillance or the use of a CHIS but, from the 1st November 2012, all applications now also require the authorisation of a Magistrate.

11.7.2 Please refer to Appendix 1 for the list of Authorising Officers, to show name, departmental details, contact number and levels of Authority.

11.7.3 The Chief Executive Officer or in her absence the Executive Director (Corporate Services) will authorise cases where confidential information is likely to be gathered or in the case of a juvenile or vulnerable CHIS.

11.7.4 The Head of Legal Practice should be informed of any changes to the list of Authorising Officers and will amend the policy accordingly. The intranet will also be updated appropriately.

11.8 Urgent Oral Authorisations

11.8.1 The provision for urgent oral authorisations is no longer available to local authorities, with effect from the 1st November 2012 as all applications now have to be put before a Magistrate for consideration. .

11.9 Local Sensitivities

11.9.1 Authorising Officers and Applicants should be aware of particular sensitivities in the local community where the directed surveillance is taking place, or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. This should form part of the risk assessment.

11.9.2 It should be noted that although this is a requirement there is no provision made within the application form for this information. Therefore applicants should cover this area where they feel it is most appropriate such as when detailing the investigation or proportionality or within the separate risk assessment form. However it must be brought to the attention of the Authorising Officer when deciding whether to authorise the activity.

11.10 Authorising Officers Responsibility

11.10.1 Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable such as where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation the Central Record of Authorisations should highlight this and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

11.10.2 Authorising Officers must treat each case individually on its merits and satisfy themselves that the authorisation is **necessary**, the surveillance is **proportionate** to what it seeks to achieve, taking into account the **collateral intrusion** issues, and that the level of the surveillance is appropriate to achieve the objectives. If any equipment such as covert cameras, video cameras are to be used the Authorising Officer should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.

11.10.3 Authorising Officers are responsible for determining when reviews of the activity are to take place.

11.10.4 Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

11.10.5 In the absence of a Line Manager or Head of Department the application should be submitted to another Authorising Officer for authorisation.

11.11 Necessity and Proportionality

11.11.1 Obtaining a RIPA authorisation will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. It must be necessary for the **prevention and detection of crime or of preventing disorder.** It must also be shown the reasons why the requested activity is necessary in the circumstances of that particular case. Can the same end result be achieved without the surveillance?

11.11.2 If similar objectives could be achieved by methods other than covert surveillance, then those methods should be used unless it can be justified why they can not be used.

11.11.3 Then, if the activities are **necessary**, the person granting the authorisation must believe that they are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the subject and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. The interference with the person's right should be no greater than that which is required to meet the aim and objectives.

11.11.4 The onus is on the Authorising Officer to ensure that the surveillance meets the tests of **necessity and proportionality**.

11.11.5 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers :

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

11.11.6 It is important that the staff involved in the surveillance and the Line Manager manage the enquiry and operation and evaluate constantly the need for the activity to continue.

11.12 Collateral Intrusion

11.12.1 Collateral intrusion is an integral part of the decision making process and should be assessed and considered very carefully by both applicants and Authorising Officers.

11.12.2 The Revised Codes state that Collateral Intrusion **is intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation such as neighbours or other members of the subject's family**. Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance activity should be carefully considered against the necessity and proportionality criteria.

11.12.3 Intended intrusion could occur if it was necessary to follow a person not committing any offences but by following this person it would lead to the person who is committing the offences.

11.12.4 Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

11.12.5 Prior to and during any authorised RIPA activity, a risk assessment should take place to identify the likely intrusion into the subject and any collateral intrusion. Officers should take continuing precautions to minimise the intrusion where possible. The collateral intrusion, the reason why it is unavoidable and the precautions taken to minimise it will have to be detailed on any relevant application forms. This will be considered by the Authorising Officer.

11.12.6 Before authorising surveillance the Authorising Officer should take into account the risk of collateral intrusion detailed on the relevant application forms as it has a direct bearing on the decision regarding proportionality.

11.12.7 The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but the authorising officer must balance this with the importance of the activity to be carried out in operational terms.

11.13 Unexpected Interference with Third Parties

11.13.1 When carrying out covert directed surveillance or using a CHIS the Authorising Officer should be informed if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. It will be appropriate in some circumstances to submit a review form and in other cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

11.14 Confidential Information

11.14.1 Confidential information consists of matters subject to Legal Privilege, confidential personal information or confidential journalistic material and applications where there is a likelihood of acquiring such information can only be authorised by the Chief Executive or the Executive Director (Corporate Services).

11.14.2 **No authorisation should be given if there is any likelihood of obtaining legally privileged material without consulting the Head of Legal Practice**.

11.14.3 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, 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. Examples might include consultations between a health professional and a patient, or information from a patient's medical records. Journalistic material is also mentioned in the codes however it is highly unlikely that this will be obtained. The definition should it be required can be obtained from the Codes of Practice at Chapter 4.

11.14.4 The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be alert to anything which may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Head of Legal Practice before further dissemination takes place;

- Confidential material should not be retained or copied unless it is necessary for specified purpose;

- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Head of Legal Practice) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information;

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

11.15 Documentation and Central Record

11.15.1 Authorising Officers or Managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process. However this will not replace the requirements under the Codes of Practice for the Council to hold a centrally held and retrievable record.

11.15.2 A centrally retrievable record of all authorisations will be held by the Head of Legal Practice and regularly updated whenever an authorisation is refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for at least three years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater, and should contain the following information:

- if refused, that the application was not authorised and a brief explanation of the reason why. The refused application should be retained as part of the Central Record of Authorisation.

- if granted, the type of authorisation and the date the authorisation was given;

- name and rank/grade of the authorising officer;

- the unique reference number (URN) of the investigation or operation;

- the title of the investigation or operation, including a brief description and names of subjects, if known;

- whether the urgency provisions were used, and if so why.

- frequency and the result of each review of the authorisation;

- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;

- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;

- the date the authorisation was cancelled.

- authorisations by an Authorising Officer in urgent cases where they are directly involved in the investigation or operation (see Authorising Officer Responsibility page 17.) If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

- the date and time when any instruction was given by the Authorising Officer.

11.15.3 As well as the Central Record the Head of Legal Practice will also retain:

- the original of each application, review, renewal and cancellation together with any supplementary documentation of the approval given by the Authorising Officer
- a record of the period over which the surveillance has taken place

11.15.4 **For CHIS applications the Codes state**;

In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

- the original authorisation form together with any supplementary documentation and notification of the approval given by the Authorising Officer;

- the original renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

- the reason why the person renewing an authorisation considered it necessary to do so;

- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;

- any risk assessment made in relation to the source;

- the circumstances in which tasks were given to the source;

- the value of the source to the investigating authority;

- a record of the results of any reviews of the authorisation;

- the reasons, if any, for not renewing an authorisation;

- the reasons for cancelling an authorisation.

- the date and time when any instruction was given by the Authorising Officer to cease using a source.

11.15.5 The Head of Legal Practice will be responsible for maintaining the Central Record of Authorisations and will ensure that all records are held securely with no unauthorised access.

11.15.6 The only persons who will have access to these documents will be the Head of Legal Practice, the Senior Responsible Officer and Authorising Officers.

11.15.7 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use made of the source.

12 Use of CCTV

12.1.1 The use of the CCTV systems operated by the Council do not normally fall under the RIPA regulations. However it does fall under the Data Protection Act 1998 and the Councils CCTV policy. However should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

12.1.2 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside law enforcement agencies such as the Police, either the CCTV staff are to have a copy of the application form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority a copy of the applicants notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been authorised. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the Information Management Team for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

12.1.3 Operators of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

13 Joint Agency Surveillance

13.1.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

13.1.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also inform the Head of Legal Practice of the unique reference number, the agencies involved and the name of the officer in charge of the surveillance. This will assist with oversight of the use of Council staff carrying out these types of operations.

14 Activities Which May Constitute Surveillance or Require Authorisation Outside of RIPA

14.1 Definition

14.1.1 Some investigative activities may not be easily recognised as constituting surveillance which requires authorisation. Any action that is likely to reveal private information1 may constitute surveillance if it includes:

- monitoring, observing, listening to persons, their movements, conversations, other activities or communications
- recording anything monitored, observed or listened to in the course of surveillance
- surveillance, by or with, assistance of a surveillance device[2]

14.1.2 This policy requires RIPA authorisation to be sought in cases where an authorisation can be sought (as per Part 3 of the Policy). Where RIPA authorisation cannot be sought, for instance where an investigation is not into a criminal offence or the offence threshold in Part 3 is not met the activity should still be authorised as per Part 6 of this policy.

14.2 Social Networks and the Internet

14.2.1 The internet is a useful investigative tool, giving access to a large amount of information which could not otherwise be obtained. The techniques and websites used change frequently and so it is difficult for definitive guidance to be written by the OSC as, by the time it is published, it may be obsolete. There is also a lack of definitive case law in this area.

14.2.2 The Chief Surveillance Commissioner comments in his 2013-14 report:

"The same considerations of privacy, and especially collateral intrusion against innocent parties, must be applied regardless of the technological advances"

14.2.3 The report clarifies (quoting from the 2011-12 annual report) that the internet is a surveillance device as per s.48(1) of RIPA and that viewing material on the internet may constitute covert surveillance as just because something is put into the public domain by someone does not mean that they expect it to be read by a public authority as "[k]nowing that something is capable of happening is not the same as an awareness that it is or may be taking place."

14.2.4 For SCDC purposes it will not be necessary to seek RIPA or non-RIPA authorisation where the activity does not constitute monitoring of material on the internet. This means that viewing material which is publically available should not require surveillance authorisation. However if repeated checks are required, for example to establish a pattern of behaviour, then this is likely to require authorisation as it will constitute monitoring.

---

[1] Private information is defined in the RIPA Codes of Practice for Covert Surveillance as: "*2.4 The 2000 Act states that private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships."*

[2] Section 48(2) Regulation of Investigatory Powers Act 2000

14.2.5 Some material may be protected from view and require the subject's authorisation in order to view it, for example by sending them a "friend request". This is likely to constitute activity which will require CHIS authorisation.

14.2.6 It is advisable for officers to take steps to protect themselves from possible reprisals. Some social networking sites make users aware of who has viewed their profile, allowing them to visit those profiles. It is not acceptable to create user profiles in false names but a separate profile should be created for work purposes which is entirely unconnected to officer's personal life and accounts.

14.2.7 It is essential that detailed notes be made by any officer viewing material on the internet explaining what they were seeking, why it was necessary and proportionate to do so and why prior authorisation was not sought.

14.2.8 Where material is printed or saved consideration must be given to the management of collateral intrusion – there may be personal data of people not subject to the investigation and this must be managed appropriately.

14.3 Visits and Observing Properties and Vehicles

14.3.1 Surveillance which is overt does not require authorisation. A visit to a property by an SCDC officer will not normally constitute surveillance if the intention is to speak to the occupier.

14.3.2 In some cases repeated visits may be made to a property in connection with an investigation and without the intention of speaking to the occupier, for example driving past the property to obtain details of vehicles or to look for signs of occupation. Such activity could become surveillance, as per 13.1 above and RIPA or non-RIPA authorisation should be sought if this is the case. This will be the case where the activity is intended to identify a pattern of behaviour, such as the presence of a vehicle at a particular location. A visit to obtain details of a vehicle is unlikely to constitute surveillance.

14.3.3 If an officer plans to conduct a visit (other than a routine visit to the occupier as per 13.3.1 above) detailed notes must be made explaining the purpose of the visit, why it is necessary and proportionate and why RIPA or non-RIPA authorisation has not been sought.

15 Annual Report to Office of Surveillance Commissioners

15.1 The Council is required to provide statistics to The Office of Surveillance Commissioners every year in March for the purposes of the OSC Annual Report. The Head of Legal Practice shall be responsible for completing the return and providing the statistics.

16 Storage and Retention of Material

16.1 All material obtained and associated with an application will be subject of the provisions of the Criminal Procedures Investigations Act 1996 (CPIA) Codes of Practice which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances. It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of the Data Protection Act. All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole

RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

16.2 Material is required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

16.3 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

16.4 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

17 Training

17.1 There will be an ongoing training programme for Council Officers who will need to be aware of the impact and operating procedures with regards to this legislation. The Head of Legal Practice will be required to retain a list of all those officers who have received training and when the training was delivered and it is for Departments to consider what their training needs are in this area.

17.2 Authorising Officers must have received formal RIPA training before being allowed to consider applications for surveillance and CHIS.

18 Oversight

18.1 Responsibilities

18.1.1 It is important that all staff involved in the RIPA application process take seriously their responsibilities. Overall oversight within the Council will fall within the responsibilities of the Senior Responsible Officer (SRO) for the Council. However careful management and adherence to this policy and procedures will assist with maintaining oversight and reduce unnecessary errors.

18.2 Reporting to Members

18.2.1 Quarterly returns of all surveillance activity undertaken by Council staff will be made to the Council's Corporate Governance Committee by the Senior Responsible Officer line with the current duties in the Codes of Practice. The Corporate Governance Committee will review the policy annually and amend the policy where necessary.

18.3 Scrutiny and Tribunal

18.3.1 Scrutiny will be provided by the Office of the Surveillance Commissioner (OSC) The Surveillance Commissioner will periodically inspect the records and procedures of the Authority to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

18.3.2 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

18.3.3 A tribunal has been established to consider and determine complaints made under RIPA if it is the appropriate forum. Persons aggrieved by conduct, e.g. directed surveillance, can make complaints. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that period.

18.3.4 Complaints can be addressed to the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H9ZQ

Appendix 1: LIST OF AUTHORISING OFFICERS AND AUTHORISING LEVELS

Alex Colyer	Interim Chief Executive & Executive Director (Corporate Services)
Mike Hill	Director (Health and Environmental Services)

Senior Responsible Officer:	Alex Colyer, Interim Chief Executive & Executive Director, Corporate Services
RIPA Monitoring Officer:	Tom Lewis, Head of Legal Practice

Appendix 2: RESOLUTION OF FULL COUNCIL

On the Council considered the revised Policy for Regulation of Investigatory Powers Act 2000 and resolved as follows:-

To adopt the revised RIPA policy with effect from 22nd September 2011

To amend the Scheme of Delegation for Officers in the Council Constitution to incorporate the changes needed to implement the revised RIPA policy.