Cambridge City Council **Item**

To:	The Leader and Executive Councillor for Strategy and Transformation: Councillor Lewis Herbert
Report by:	Head of Legal Services/ Monitoring Officer
Relevant scrutiny committee:	Strategy & Resources Scrutiny Committee 9/1/2015
Wards affected:	All

REVIEW OF USE OF THE REGULATION OF INVESTIGATORY POWERS ACT
Not a Key Decision

1. Executive summary

1.1 A Code of Practice introduced in April 2010 recommends that councillors should review their authority's use of the Regulation of Investigatory Powers Act 2000 (RIPA) and set its general surveillance policy at least once a year. The Executive Councillor for Community Development and Health and Community Services Scrutiny Committee last considered these matters on 20 January 2014.

1.2 The City Council has not used surveillance or other investigatory powers regulated by RIPA since February 2010.

1.3 This report sets out the Council's use of RIPA and the present surveillance policy.

2. Recommendations

The Executive Councillor and Scrutiny Committee are recommended:

2.1 To review the Council's use of RIPA set out in paragraph 5.1 of this report.

2.2 To note and endorse the steps described in paragraph 5.1 and in Appendix 1 to ensure that surveillance is only authorised in accordance with RIPA.

The Executive Councillor is recommended:

To approve the amended general surveillance policy in Appendix 1 to this report.

3. Background

3.1 The Regulation of Investigatory Powers Act imposes controls on the circumstances in which public bodies can use covert investigative methods in connection with their statutory functions. Local authorities may only use these methods for the purpose of preventing or detecting crime or of preventing disorder.

3.2 These are the activities that are regulated by RIPA:

a) Covert directed surveillance

Surveillance is “covert” if it is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. It is “directed” if it is undertaken for the purposes of a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about a person. Surveillance is not directed if it is an immediate response to events or circumstances; for instance if a police officer sees someone acting suspiciously and decides to follow them. The Council uses covert directed surveillance very sparingly – and has not used it at all in the period covered by this report.

b) Covert human intelligence source (“CHIS”)

A covert human intelligence source is someone who establishes or maintains a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informer or Council officer to strike up a relationship with someone as part of an investigation to obtain information “under cover”. The Council has never authorised the use of a “covert human intelligence source” under RIPA.

c) Access to Communications Data

There are stringent controls placed on access by the Council to “communications data”. The Council is not entitled to obtain access to the content of communications between third parties but can, in some circumstances, obtain information relating to the use of a communications service. “Communications services” include telecom

providers, postal services and internet service providers. The Council has never authorised access to communications data under RIPA.

3.3 More detail of the nature of the scope of RIPA and controls and procedures are set out in the general surveillance policy in Appendix 1.

4. Member Supervision of the Use of RIPA

4.1 A Home Office Code of Practice provides for a wider supervisory role for councillors. The code states that, at least once a year, councillors should review the Council's use of RIPA and set the general surveillance policy. This report gives members this opportunity.

4.2 Councillors should also consider internal reports on the use of RIPA at least on a quarterly basis to ensure that it is being used consistently as per the council's policy and that the policy remains fit for purpose. The Code emphasises that councillors should not be involved in making decisions on specific authorisations. In fact, since the Code of Practice came into effect, the Council has not used RIPA powers, so there has been no occasion to issue a report.

5. The Council's Use of RIPA

5.1 The City Council is very sparing in its use of RIPA powers. In fact, it has not authorised the use of RIPA powers in the period covered by this report (January 2013 to January 2014) and not used these powers since February 2010.

5.2 As mentioned in Section 3, the Council has never used RIPA powers to authorise the use of "confidential human intelligence sources" or the powers relating to the obtaining of communication data.

5.3 When members previously reviewed the Council's use of RIPA, they asked for information about surveillance etc. carried out by the Council under an authorisation given by a third party. This might arise where an investigation is being led by another agency (e.g. Police or HMRC) and the Council is asked to assist. There have been no instances of this since the date of the last report.

6. The Protection of Freedoms Act 2012

6.1 From 1 November 2012, all local authority surveillance authorised under the Regulation of Investigatory Powers Act 2000 (RIPA) has been subject to approval by a Magistrate.

6.2 Approval can only be given if the Magistrate is satisfied that:

(a) There were reasonable grounds for the authorising officer approving the application to believe that the Directed Surveillance or deployment of a Covert Human Intelligence Source (CHIS) was necessary and proportionate and that there remain reasonable grounds for believing so.

(b) The authorising officer was of the correct seniority within the organisation i.e. a Director, Head of Service, Service Manager or equivalent.

(c) The granting of the authorisation was for the prescribed purpose, which is preventing or detecting crime or disorder and, in the case of directed surveillance, is confined to cases where the offence under investigation carries a custodial sentence of six months or more.

6.3 There are also additional safeguards in relation to the use of a CHIS. (As mentioned in paragraph 3.2, The Council has never authorised the use of a "covert human intelligence source" under RIPA.)

7. The Council's Surveillance Policy

7.1 The Council's surveillance policy is set out at Appendix 1. It sets out the tests to apply in determining whether the use of RIPA powers is necessary and proportionate.

7.2 The Council's surveillance policy needs to be updated to take account of the development of social media and the potential for infringing privacy through accessing this in the course of investigations.

7.3 The most recent annual report of the Chief Surveillance Commissioner draws attention to this. The report says:

"This is now a deeply embedded means of communication between people and one that public authorities can exploit for investigative purposes. I am reasonably satisfied that there is now a heightened awareness of the use of the tactic and the advisable authorisations under RIPA that should be considered. Although there remains a significant debate as to how anything made publicly available in this medium can be considered private, my Commissioners remain of the view that the repeat viewing of individual "open source" sites for the purpose of intelligence gathering and data collation should be considered within the context of the protection that RIPA affords to such activity."

7.4 A very recent revised version of the Home Office's Code of Practice on Covert Surveillance and Property Interference came into force on 10 December 2014. This also gives guidance. It says:

"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 a public authority 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 as set out elsewhere in this Code. Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered."

7.5 The Council's RIPA Code of Practice has been amended to address this issue. Where individuals publish information freely (e.g. twitter accounts, LinkdIn profiles), there is unlikely to be any interference with privacy rights or any RIPA issues. This is also likely to be the case with other information published openly on the Internet. Care should, however, be taken with other social media, such as Facebook. Even if the user has not used privacy settings to restrict access, this does not necessarily mean that they have made a decision to publish personal information to the world. It is likely to be proportionate, in connection with an investigation to make a single visit to an unsecured Facebook profile. Further visits could amount to surveillance and may require authorisation

7.6 The Head of Legal Services has alerted directors and service heads to this issue. The only instance in which officers look at information on social media is in relation to criminal investigations conducted by the fraud prevention team. This is confined to viewing a published profile once and repeat visits are not made. The Head of Legal Services regards this as proportionate, given the importance of investigating fraud, and as not requiring RIPA authorisation.

7.7 In addition to the new text on social media, the amendments include a section drawing specific attention to the steps that need to be taken in relation to surveillance not covered by RIPA, as well as some updating.

7.8 The Executive Councillor is asked to endorse the policy incorporating the proposed amendments

8. Implications

a) **Financial Implications** - None

(b) **Staffing Implications** - None

(c) **Equality and Poverty Implications**

A formal equality impact assessment has not been carried out in preparing this report. Equality impact issues are addressed, and safeguards contained, within the body of the general surveillance policy which the Executive Councillor is being asked to endorse. Paragraph 9.5 of the policy highlights the need to consider equality issues as part of considering whether to use RIPA powers. Paragraph 9.7 highlights the special care needed if surveillance might involve obtaining access to religious material. The Head of Legal Services receives copies of all authorisations and takes an overview of the use of RIPA. The member supervision outlined in section 4 of this report would also help ensure that the policy is being applied properly.

(d) **Environmental Implications**

The proposals in this report have a “nil” climate change impact.

(e) **Procurement** - None

(f) **Consultation and communication**

The RIPA general surveillance policy is based on legal requirements and the guidance contained in Home Office codes of practice and there has been no external consultation on this.

(g) Community Safety

Although the Council’s use of RIPA has been very sparing, there have been, and will be, occasions on which the use of the powers are justified and necessary to ensure community safety.

9. Background papers

These background papers were used in the preparation of this report:

Report to the Leader and Strategy and Resources Scrutiny Committee: Review Of Use Of The Regulation Of Investigatory Powers Act (20 January 2014)

ANNUAL REPORT of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014. This is a published source available at https://osc.independent.gov.uk/wp-content/uploads/2014/09/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf

6. Appendix

City Council RIPA Procedure Guide with proposed amendments.

7. Inspection of papers

To inspect the background papers or if you have a query on the report please contact:

Author's Name: Simon Pugh
Author's Phone Number: 01223 - 457401
Author's Email: simon.pugh@cambridge.gov.uk

Appendix 1 - Cambridge City Council

The Regulation of Investigatory Powers Act 2000: A procedure guide on the use of covert surveillance and "covert human intelligence sources"

Statement of Intent: Cambridge City 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 Code.

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 there is a clear public interest justification.

2. What does RIPA do?

2.1 RIPA places controls on the use of certain methods of investigation. In particular, it regulates the use of surveillance and "covert human intelligence sources". This guide covers these aspects of the Act. Further guidance will be issued on other aspects of the Act if necessary.

2.2 RIPA's main implications for the Council are in respect of covert surveillance by Council officers and the use of "covert human intelligence sources". (A covert human intelligence source is someone who uses a relationship with a third party in a secretive manner to obtain or give information – for instance an informer or someone working "under cover".)

3. Some definitions

"*Article 8 Rights*

This refers to the rights of individuals under the European Convention on Human Rights:

"Everyone has the right to respect for his private and family life, his home and his correspondence.

"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The Council must not infringe these rights unless they are acting in accordance with the law for one of the purposes mentioned in the

second paragraph. Even then, any infringement of this right needs to be proportionate. (See paragraph 9.4.)

3.1 *"Covert"*

Concealed, done secretly

3.2 *"Covert surveillance"*

Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

3.3 *"Directed surveillance"*

Directed surveillance is defined in RIPA as surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or operation;

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

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance (i.e. where the circumstances make it impractical to seek authorisation. An example might be where a police officer on patrol sees a person acting suspiciously and decides to watch them surreptitiously to see whether they are intending to commit a crime.)

Private information in relation to a person includes any information relating to his private or family life.

3.4 *"Intrusive surveillance"*

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

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

b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

4. RIPA and Surveillance – what is not covered

4.1 General observation forms part of the duties of some Council officers. They may, for instance, be on duty at events in the City and will monitor the crowd to maintain public safety and prevent disorder. Environmental Health Officers might covertly observe and then visit a shop as part of their enforcement function. Such observation may involve the use of equipment merely to reinforce normal sensory

perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of RIPA.

4.2 Neither do the provisions of the Act cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. (There is a separate Code of Practice adopted by the Council to govern use of CCTV. For information about this, contact Martin Beaumont, CCTV Manager.)

5. RIPA and Surveillance – What is covered?

5.1 The Act is designed to regulate the use of "covert" surveillance. Covert surveillance means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. Strictly speaking, only two types of covert surveillance are regulated by RIPA – "directed" and "intrusive" surveillance. However, where the purpose of a surveillance operation is to obtain private information about a person, the authorisation procedures set out in this guide should be followed and the surveillance treated as being "directed".

6. What is "directed surveillance"?

6.1 Directed surveillance is defined in RIPA as surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or operation;

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

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance. (See the clarification of this in paragraph 3.3.)

Private information in relation to a person includes any information relating to his private or family life.

6.2 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a plain clothes police officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of a patrol.

6.3 Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. Such activity is defined as "intrusive surveillance" and is dealt with in paragraph 7.

6.4 In practice, the sort of directed surveillance which the Council might undertake would include the use of concealed cameras as part of an investigation into antisocial behaviour or breach of tenancy conditions. It might include covert surveillance connected with the enforcement of environmental health or planning regulations or in connection with investigating benefit fraud. You should treat anything involving the use of concealed cameras or anything involving keeping covert observation on premises or people as potentially amounting to directed surveillance. If you are unsure, please take advice either from your manager or supervisor, or from the Head of Legal Services.

6.5 Directed surveillance **must** be properly authorised in accordance with the procedure set out in section 9.

6.6 You should treat any covert surveillance which is likely to intrude upon anyone's privacy to more than a marginal extent as directed surveillance, even if it does not fall within the strict terms of the definition – for instance where surveillance is not part of a specific investigation or operation.

New Section 7. Directed Surveillance and Social Media

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 you intend to use the internet as part of an investigation, you 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. (See Section 3 for an explanation of Article 8 rights.)

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. If your proposed use of social media in connection with an investigation amounts to covert directed surveillance within the scope of RIPA by electronic means, an authorisation in accordance with the procedure set out in section 9. Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered.

Where individuals publish information freely (e.g. twitter accounts, LinkdIn profiles), there is unlikely to be any interference with Article 8 rights. This is also likely to be the case with other information published openly on the Internet. Care should be taken with other social media, such as Facebook. Even if the user has not used privacy settings to restrict access, this does not necessarily mean that they have made a decision to publish personal information to the world. It is likely to be proportionate, in connection with an investigation (e.g. benefit fraud) to make a single visit to an unsecured Facebook profile. Further visits could amount to surveillance. If you are considering monitoring social media such as Facebook in connection with an investigation. you should first seek advice on whether RIPA authorisation is needed.

[Then renumber.]

7. What is intrusive surveillance?

7.1	**An important warning: the Council cannot authorise intrusive surveillance.**

7.2 Intrusive surveillance is defined as covert surveillance that:

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

b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

7.2 In essence, intrusive surveillance amounts to intrusion into people's homes or vehicles either physically or by means of a surveillance device.

7.3 **Intrusive surveillance cannot be undertaken without authorisation and the Council cannot authorise intrusive surveillance.** Bodies such as the Police and Customs and Excise can authorise intrusive surveillance. If you are asked by another agency to co-operate with intrusive surveillance, you should seek advice from the Head of Legal Services immediately. Where other authorities say that they are authorised to undertake intrusive surveillance but need our co-operation, we need to check that their authorisation is in order.

8. What is a covert human intelligence source?

8.1 A covert human intelligence source is someone who establishes or maintains a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informer or Council officer to strike up a relationship with someone as part of an investigation to obtain information "under cover".

8.2 Someone who volunteers information to the Council, either as a complainant (for instance, about anti-social behaviour or a breach of planning regulations) or out of civic duty, is unlikely to be a covert human intelligence source. If someone is keeping a record, say, of neighbour nuisance, this will not amount by itself to use of a covert human intelligence source. However, if we are relying on, say, a neighbour to ask questions with a view to gathering evidence, then this may amount to use of a covert human intelligence source.

8.3 The use by the Council of covert human intelligence sources is expected to be extremely rare and, for that reason, this guide does not deal with the issues to which they give rise. If you are contemplating use of a covert human intelligence source, please take advice from the Head of Legal Services before putting your plan into action.

9. Authorising Directed Surveillance: The Rules

9.1 It is crucial that all directed surveillance is properly authorised. Failure to secure proper authorisation and to comply with this procedure could lead to evidence

being excluded by the courts and to complaints against the Council. The Council is subject to audit and inspection by the Office of the Surveillance Commissioner and it is important that we can demonstrate compliance with RIPA and with this code. **Again, please note that the Council cannot authorise intrusive surveillance – see section 7.**

9.2 **Who can authorise directed surveillance?** Regulations made under the Act say that the most junior level at which authorisations can only be given is by what it refers to as "assistant chief officers". For the purposes of this Code, authorisations may only be given by the officers identified in the Appendix to this Guide referred to as "authorising officers". In cases of urgency, if it is not possible to seek authority from an authorising officer, authority may be given by a deputy to an authorising officer, but ratification of that authority should be sought at higher level as soon as practical, and the reasons for urgency recorded on the authorisation form. Where practical, the authorising officer should not be directly involved in the case giving rise to the request for authorisation. (However, an authorising officer may authorise a request made by staff who report to them if they are not directly involved in the case.) Where it is not practical for authorisation to be given by an officer who is not directly involved, this should be noted with reasons on the authorisation form. In addition to internal authorisation, directed surveillance cannot be carried out without the approval of a Magistrate. (See paragraph 10.2 below.)

9.3 **On what grounds can directed surveillance be authorised?** Directed surveillance can only be authorised by local authorities:

- for the purpose of preventing or detecting serious crime where the offence under investigation carries a custodial sentence of six months or more.

When the legislation was introduced, the Council could authorise directed surveillance on other grounds (e.g. in the interests of public safety or in the interests of protecting public health, or to prevent or detect disorder) but the serious crime ground is the only one available to local authorities. The Police have wider powers to authorise directed surveillance.

Please note that surveillance has to be **necessary** for the serious crime purpose. If you can just as well carry out an investigation by means which do not involve directed surveillance, then you should use them.

9.4 **Is the proposed surveillance proportionate?** Authorisation should not be sought, and authority should not be given unless you are satisfied that the surveillance is proportionate. You should make sure that any interference with privacy is justified by the end being sought. Unless the benefit to be obtained from surveillance is significant, and unless the problem you are seeking to tackle is serious, the use of surveillance is unlikely to be proportionate. We should not "use a sledgehammer to crack a nut"!

9.5 **Is the proposed surveillance discriminatory?** The Council is under a legal obligation to avoid either direct or indirect discrimination in carrying out its functions. As surveillance can interfere with rights contained in the European Convention on Human Rights, discrimination can also amount to a breach of the Human Rights Act. You should be sensitive to this issue and ensure that you apply similar standards to seeking or authorising surveillance regardless of ethnic origin, sex or sexual orientation, disability, age etc. You should be alert to any

assumptions about people from different backgrounds which may not even be consciously held.

9.6 **Might the surveillance involve "collateral intrusion"?** In other words, might the surveillance intrude upon the privacy of people other than those who are the subject of the investigation. You should be sensitive of the privacy rights of third parties and consider very carefully whether the intrusion into their privacy is justified by the benefits of undertaking the surveillance.

9.7 **Might the surveillance involve acquiring access to any confidential or religious material?** If so, then the surveillance will require a particularly strong justification and arrangements need to be put in place to ensure that the information obtained is kept secure and only used for proper purposes. Confidential material might include legal or financial records, or medical records. Where there is a possibility that access to confidential or religious material might be obtained, the authorisation of the Chief Executive (or, in her absence in cases where it is not practical to wait for her return, the authorisation of a Director acting as her deputy) should be sought.

10. Authorising Directed Surveillance: The Procedure

10.1 **Applying for authorisation.**

10.1.1 Detailed guidance on the authorisation procedure and on how to complete the statutory forms is available on the Council's Intranet at http://intranet/Guidelines/Docs/RIPA%20Guidance%20Manual.pdf The individual forms are available separately and links to them are set out in Appendix 3. You must only use the forms that are on the Intranet, you should read the accompanying notes carefully and follow them when completing the form.

10.1.2 Before submitting an application for authorisation, you must supply a copy of your request to the Head of Legal Services. You may only submit your application for authorisation if you obtain the approval of the Head of Legal Services.

10.1.3 A written application for authorisation for directed surveillance should describe in detail any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;

- the details of any potential collateral intrusion and why the intrusion is justified;

- the details of any confidential information that is likely to be obtained as a consequence of the surveillance.

- the level of authority required (or recommended where that is different) for the surveillance; and

- a subsequent record of whether authority was given or refused, by whom and the time and date.

10.1.4 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given; and/or

- the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

10.1.5 Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

10.2 Approval by a Magistrate

10.2.1 The internal authorisation for covert surveillance is not to take effect until a Magistrate has made an order approving it. Approval can only be given if the Magistrate is satisfied that:

(a) There were reasonable grounds for the authorising officer to believe that the directed surveillance was necessary and proportionate and that there remain reasonable grounds for believing so.

(b) The authorising officer was of the correct seniority within the organisation i.e. a Director, Head of Service, Service Manager or equivalent.

(c) The granting of the authorisation was for preventing or detecting crime and that the offence under investigation carries a custodial sentence of six months or more.

10.2.2 You must not commence covert surveillance until you have confirmation that the Magistrate's approval has been given.

10.3 **Duration of authorisations**

10.3.1 A written authorisation granted by an authorising officer will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

10.3.2 Urgent oral authorisations or written authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after **seventy-two hours**, beginning with the time when the authorisation was granted or renewed. This will apply to written authorisations given by deputies to Heads of Services.

10.3.3 Even though authorisations cease to have effect after three months, you should not simply leave them to run out. When the surveillance ceases to be necessary, you should always follow the cancellation procedure. See section 10.6. Where surveillance has ceased, we must be able to match each authorisation with a cancellation.

10.4 **Reviews**

10.4.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The maximum period between authorisation and review, and between reviews, should be four weeks. The more significant the infringement of privacy, the more frequent should be the reviews. The results of a review should be recorded on the central record of authorisations (see paragraph 11). Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

10.4.2 In each case authorising officers within the Council should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

10.4.3 A link to the form to record a review of an authorisation may be found in Appendix 2 to this Guide.

10.5 **Renewals**

10.5.1 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, s/he may renew it in writing for a further period of **three months**. A single renewal may also be granted orally in urgent cases and may last for a period of **seventy-two hours**. A renewal cannot take effect unless it has been approved by a Magistrate. If you think a renewal might be needed, you should plan to allow sufficient time for an application to a Magistrate to be made before expiry.

10.5.2 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations (other than oral authorisations in urgent cases) may be renewed more than once, provided they continue to meet the criteria for authorisation.

10.5.3 All applications for the renewal of an authorisation for directed surveillance should be made on the form linked to Appendix 2 to this guide and should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

- any significant changes to the information given in the original application for authorisation;

- the reasons why it is necessary to continue with the directed surveillance;

- the content and value to the investigation or operation of the information so far obtained by the surveillance;

- the results of regular reviews of the investigation or operation.

10.5.4 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations (see paragraph 12).

10.6 **Cancellations**

10.6.1 The authorising officer who granted or last renewed the authorisation must cancel it if he is 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. If in doubt about who may cancel an authorisation, please consult the Head of Legal Services. Cancellations are to be effected by completion of the form linked to in Appendix 2 to this Guide.

10.6.2 **N.B. Please note the warning in paragraph 10.3.3 that there must be a completed cancellation for each authorisation once surveillance has been completed. An authorisation cannot simply be allowed to expire.**

10.7 **Ceasing of surveillance activity**

10.7.1 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be included in the Notification of Cancellation form.

11. Record Keeping and Central Record of Authorisations

11.1 In all cases in which authorisation of directed surveillance is given, the Service Head is responsible for ensuring that the following documentation is kept safely for a period of at least three years from the date of authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;

- a record of the period over which the surveillance has taken place;

- the frequency of reviews prescribed by the authorising officer;

- a record of the result of each review of the authorisation;

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

- the date and time when any instruction was given by the authorising officer.

11.2 In addition, copies the following must be sent to the Head of Legal Services immediately upon completion:

- all completed forms authorising directed surveillance;

- all completed forms authorising renewal of directed surveillance;

- all completed forms cancelling directed surveillance.

These will be kept by the Head of Legal Services who will review them at least every twelve months in his capacity as the Council's Monitoring Officer.

12. Authorising Use of Covert Human Intelligence Sources

12.1 Similar principles and procedures apply to authorising the use of covert human intelligence sources, including the need for authorisations to be approved by a Magistrate. If it becomes apparent that their use is more than very exceptional, detailed guidance will be published and circulated. For the present, officers' attention is drawn to the explanation of the nature of a covert human intelligence source in Paragraph 9. If you think you might be using, or might use, a covert human intelligence source, please contact the Head of Legal Services, who will advise on the principles to be applied, the authorisation procedure, record keeping etc. For the avoidance of doubt, the Council will comply, so far as applicable, with the model guidance issued by the Home Office.

13. Authorisations by Third Parties

13.1 You may be approached by another agency, e.g. the Police or HMRC, to co-operate in undertaking activities regulated by RIPA. In cases where the City Council is acting on behalf of another agency, the tasking agency should normally obtain and provide evidence of the RIPA authorisation. Although the Council can act on an authorisation obtained by another agency, it is still important for the Council to reach a view on whether it is appropriate to co-operate. Please, where practical, seek the advice of the Head of Legal Services before acting on a third-party authorisation.

13.2 Home Office guidance says that, where possible, public authorities should seek to avoid duplication of authorisations as part of a single investigation or operation. For example, where two agencies are conducting directed surveillance as part of a joint operation, only one authorisation is required. Duplication of authorisations does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on authorities. But we should not use Police authorisation as a means to avoid the safeguards put in place for local authority use of RIPA or as a means of carrying out surveillance for purposes not authorised for local authorities; e.g. intrusive surveillance or surveillance for non-permitted purposes. If it is primarily a Council operation, then the Council should be responsible for authorisation.

13.3 You must notify the Head of Legal Services of all occasions on which you act under a RIPA authorisation obtained by a third party.

14. Access to Communications Data

14.1 There are stringent controls placed on access by the Council to "communications data". The Council is not entitled to obtain access to the content of communications between third parties but can, in some circumstances, obtain information relating to the use of a communications service. "Communications services" include telecom providers, postal services and internet service providers.

14.2 This is a complex area, procedurally and legally. Access to communications data can only be obtained through the Council's designated "single point of contact" ("SPOC") for communications data. The Head of Legal Services has this role and you should consult him at an early stage if you think you may need access to communications data.

15. Covert surveillance outside of RIPA

15.1 Not all types of covert surveillance falls within the scope of RIPA which, for local authorities, is limited to criminal investigations. On occasion, it may be appropriate to carry out covert surveillance in connection with, for instance, an audit or disciplinary investigation. Formal RIPA authorisation will not be needed in these circumstances but the principles embodied in RIPA still apply. In these circumstances, you should complete the non-RIPA application form and submit it to an authorising officer for approval. Detailed guidance on non-RIPA surveillance is available on the Intranet at http://live.drupal.intranet.ccc.local/content/regulation-investigatory-powers-act-2000 .

15. Further Information

15.1 Departments may wish to develop their own guidance and Environmental Health and Waste Management has already done so. This is to be encouraged. However, the principles and procedures contained in departmental guidance must be compatible with this guidance.

15.2 There is much helpful information on the Home Office web site about RIPA. See Appendix Two for links.

15.3 The Head of Legal Services is happy to advise further on issues connected with RIPA. Departments need to consider what their training needs are in this area and the Head of Legal Services is willing to discuss what help he can offer with this.

Simon Pugh
Head of Legal Services

Approved Authorising Officers for the Purposes of the Regulation of Investigatory Powers Act 2000

- Liz Bisset, Director of Community Services
- Robert Hollingsworth, Head of City Homes
- Jas Lally, Head of Refuse and Environmental ~~Services~~

The Leader of the Council delegated power to the Chief Executive to designate authorised officers for the purposes of Chapters II and III of the Act. (Record of Decision ref: 07/S&R/14, 3 September 2007.

Links

Links to Home Office Information on RIPA, including codes of practice are at http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ Forms are also available via this site but you should only use the forms on the Council's Intranet, which may be found through the links in Appendix Three.

Intranet Guidance

RIPA Covert Surveillance Forms and Guidance

Regulation of Investigatory Powers Act 2000

Guidance on the use of covert surveillance and "covert human intelligence sources"

- The Regulation of Investigatory Powers Act 2000 - Procedure Guide 2013 [DOC, 87kB]

The guidance manual and the information set out in all the forms below have been purchased from an external source and copyright belongs to Ibrahim Hasan (2010) of Act Now Training - www.actnow.org.uk - Surveillance Law Training and Resources. Under no circumstances should copies of the manual or guidance be provided to any other person or organisation outside Cambridge City Council.

RIPA Guidance Manual

- 1. Introduction [PDF, 0.5MB]
- 2. Guidance for Authorising Officers [PDF, 153kB]
- 3. Completing the RIPA Forms [PDF, 0.8MB]
- 4. Seeking Magistrates' Approval [PDF, 121kB]
- 5. Non RIPA Surveillance [PDF, 0.6MB]

Directed Surveillance (DS) Forms

- 15 DS Review Form.doc [DOC, 61kB]
- 14 DS Application Form.doc [DOC, 115kB]
- 17 DS Cancellation Form.doc [DOC, 47kB]
- 16 DS Renewal Form.doc [DOC, 59kB]

Covert Human Intelligence Source (CHIS) Forms

- Completing the CHIS Forms.doc [DOC, 24kB]
- CHIS Review [DOC, 62kB]

- CHIS Application [DOC, 122kB]
- CHIS Cancellation [DOC, 45kB]
- CHIS Renewal [DOC, 61kB]
- CHIS Non-RIPA Form [DOC, 89kB]

~~RIPA Guidance Manual (PDF)~~

~~Directed Surveillance (DS) Review (Word)~~

~~DS Application (Word)~~

~~DS Cancellation (Word)~~

~~DS Renewal (Word)~~

~~Completing the CHIS (Covert Human Intelligence Source) Forms (Word)~~

~~CHIS Review (Word)~~

~~CHIS Application (Word)~~

~~CHIS Cancellation (Word)~~

~~Covert Human HIS Renewal (Word)~~