Philip

Cambridge City Council

To:	Executive Councillor for Community Development and Health: Councillor Tim Bick
Report by:	Head of Legal Services
Relevant scrutiny committee:	Community Services Scrutiny Committee 13/10/2011
Wards affected:	All Wards

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

1.2 The report also sets out some planned changes to the RIPA regime.

1.3 Finally, the report seeks authority to enter into a protocol with Cambridgeshire Police governing co-operation provided by the City Council to the Police when the latter uses RIPA powers.

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:

2.3 To approve the general surveillance policy in Appendix 1 to this report; and

2.4 To authorise the Director of Environment to enter into the protocol in Appendix 2 of this report.

2.5 To confirm that the Council's Monitoring Officer should act as the Council's Senior Responsible Officer for RIPA purposes.

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:

1. 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 – on only one occasion in the last three years.

2. Covert human intelligence source

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.

3. 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.

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 new 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 authorised use of RIPA powers on only one occasion since October 2008 – in February 2010. The authorisation on that occasion was for directed surveillance by covert CCTV as part of co-operation with a Police investigation into incidents of serious domestic assault. Covert CCTV was installed in the victim's home with her full co-operation to gather evidence against the perpetrator. Whilst the officers were satisfied that the surveillance was appropriate in supporting the victim and in gathering evidence of serious criminal behaviour, the Police, rather than the City Council should have authorised the surveillance. Technically, this amounted to intrusive surveillance, which the Police can authorise, but the Council cannot. The guidance has been strengthened to emphasise this by ensuring

that applications are scrutinised by the Head of Legal Services before they are considered by an authorising officer.

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 The Protection of Freedoms Bill contains measures further to ensure that RIPA powers are used appropriately. The Bill provides that a magistrate will need to approve use of RIPA powers.

5.4 The Office of Surveillance Commissioners carried out an inspection of the Council's RIPA policy and procedures in April 2010. The report comments on the authorisation of intrusive surveillance described in paragraph 5.1, but it is in other respects positive about the Council's approach to RIPA. Copies of the report are available from the Head of Legal Services, subject to redaction of an appendix which contains personal information about a third party.

6. The Council's Surveillance Policy.

6.1 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. The Executive Councillor is asked to endorse the policy.

7. CCTV Protocol

7.1 Cambridgeshire Police have been working with the City Council and other Cambridgeshire authorities to agree a protocol for the use of CCTV during Police surveillance operations. The proposed protocol is set out in Appendix 2. It "is intended to provide a framework for Cambridgeshire Constabulary and Local Authorities utilising CCTV systems within the County to work together under the Regulation of Investigatory Powers Act 2000… to conduct certain types of surveillance during planned or unplanned investigations and to give a common practice direction to all concerned."

7.2 The use of surveillance by Cambridgeshire Police is also regulated by RIPA. The main differences between the City Council and the Police with regard to surveillance are:

a) The City Council may only use RIPA powers for the prevention and detection of crime and disorder, but the Police can use RIPA powers in a much wider range of circumstances.

b) The Police can authorise intrusive surveillance, which the City Council cannot.

7.3 The use of overt CCTV cameras does not normally require authorisation under RIPA. Members of the public will be aware that such systems are in use, and their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008, issued by the Information Commissioner's Office.

7.4 However, where overt CCTV are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, this is likely to amount to directed covert surveillance which would require authorisation under RIPA.

7.5 It will be the responsibility of the Police to obtain authorisation for directed surveillance and the protocol places them under an obligation to disclose their authorisation when requesting use of CCTV cameras for this purpose.

7.6 It is important to note that the protocol will not oblige the City Council to provide Police access to CCTV cameras for covert surveillance purposes. The Council's CCTV Code of Practice says:

"The Regulation of Investigatory Powers Act is to ensure that investigatory powers of the intelligence services, the police and other enforcement agencies are used in accordance with the Human Rights Act and Cambridge City Council will ensure that all requests for assistance from the Council's CCTV system under this Act are examined in detail to ensure that they are proportionate, legal, appropriate and necessary. Where any doubts exist, legal advice or advice from the Surveillance Commissioner's Office (address on last page of this document) will be sought before the Council agrees to undertake action under this Act."

7.7 The Executive Councillor is asked to authorise the Director of Environment to enter into the protocol on behalf of the Council.

8. The Senior Responsible Officer

8.1 A Home Office Code of Conduct introduced in April 2010 recommends that the Council designates a "senior responsible officer" (SRO) in relation to RIPA powers and obligations.

8.2 The SRO is responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance;
- compliance with the Act and with the Codes
- engagement with the OSC inspectors when they conduct their inspections, where applicable, and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

8.3 The Code recommends that the SRO should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in the light of any recommendations in OSC inspection reports. Where a report highlights concerns about the standard of authorising officers, the SRO will be responsible for ensuring the concerns are addressed.

8.4 The Head of Legal Services/Monitoring Officer has been carrying out this role and the Executive Councillor is asked to confirm this designation.

9. Implications

(a) **Financial Implications** There are no financial implications.

(b) **Staffing Implications** There are no staffing implications.

(c) **Equal Opportunities 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 increased role for 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) **Consultation**

The protocol in Appendix 2 is the product of consultation between the Police and Cambridgeshire local authorities. 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.

(f) **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.

5. Background papers

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

Report to Strategy Scrutiny Committee, 1 September 2008: “Regulation Of Investigatory Powers Act 2000”

Office of Surveillance Commissioners Inspection Report: April/May 2010 (excluding the Appendix).

A Code Of Practice For Cambridge City Council’s Public CCTV Scheme

6. Appendices

Appendix 1: City Council RIPA Procedure Guide

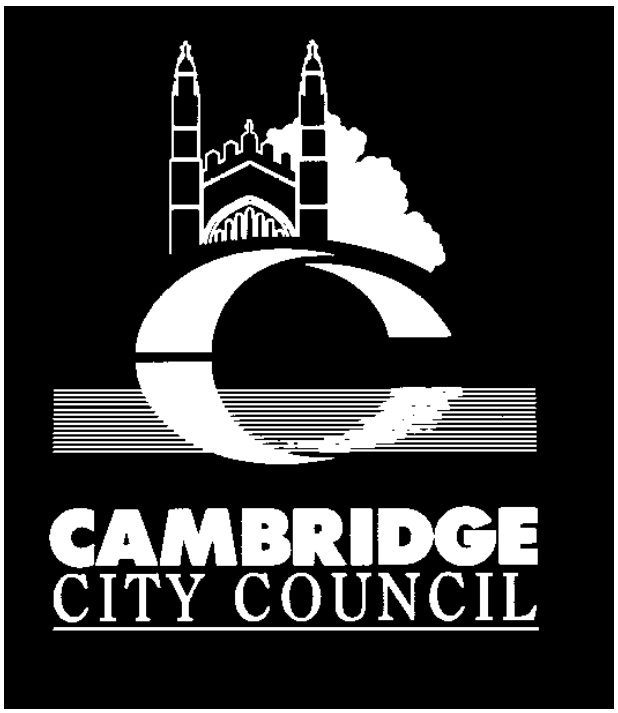
Apendix 2: Protocol between Cambridgeshire Constabulary and Local Authority CCTV Partners for the use of Public Authority CCTV systems during surveillance operations conducted by Cambridgeshire Constabulary

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



THE REGULATION OF INVESTIGATORY POWERS ACT 2000

A procedure guide on the use of covert surveillance and "covert human intelligence sources"

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

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, Facilities and 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.

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.

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 crime or of preventing disorder;

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) but the crime and disorder 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 crime and disorder 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 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 When applying for authorisation, you should copy your request to the Head of Legal Services, who is responsible for keeping a central record of RIPA authorisations and also for taking an overview of the Council's use of RIPA.

10.1.2 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.

10.1.3 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.

10.1.4 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 **Duration of authorisations**

10.2.1 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.

10.2.2 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.

10.2.3 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 10.5. Where surveillance has ceased, we must be able to match each authorisation with a cancellation.

10.3 **Reviews**

10.3.1 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.

10.3.2 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.

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

10.4 **Renewals**

11.4.1 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**.

10.4.2 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.

10.4.3 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.

10.4.4 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).

10.5 **Cancellations**

10.5.1 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.

N.B. Please note the warning in paragraph 10.2.3 that there must be a completed cancellation for each authorisation once surveillance has been completed. An authorisation cannot simply be allowed to expire.

10.6 **Ceasing of surveillance activity**

10.6.1 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. 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. Access to Communications Data

13.1 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.

13.2 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.

14. Further Information

14.1 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.

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

14.3 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

Appendix One: 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
- Simon Pugh, Head of Legal Services
- Jas Lally, Head of Environmental Services

The Leader of the Council has 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.

Appendix Two

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.

Appendix Three

RIPA Covert Surveillance Forms and Guidance

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)

Appendix 2

Creating a safer
Cambridgeshire

Protocol between Cambridgeshire Constabulary and Local Authority CCTV Partners for the use of Public Authority CCTV systems during surveillance operations conducted by Cambridgeshire Constabulary

1. Introduction

1.1 This protocol is intended to provide a framework for Cambridgeshire Constabulary and Local Authorities utilising CCTV systems within the County to work together under the Regulation of Investigatory Powers Act 2000 (hereafter referred to as 'the Act') to conduct certain types of surveillance during planned or unplanned investigations and to give a common practice direction to all concerned. It must be stressed that this protocol is meant to work with agency's existing policy and procedures.

1.2 It is an underlying principle of this document that each investigation will be considered on a case by case basis, and will be assessed on its individual merits.

1.3 Further guidance is available in 'The Covert Surveillance and Property Interference Revised Code of Practice' issued under Section 71 of the Act (hereafter known as 'the Code of Practice).

1.4 The consequences of not obtaining an authorisation under Part 2 of the Act may be that where there is an interference by a public authority with rights under Article 8 of the Human Rights Act 1998 (invasion of privacy), and there is no other lawful source of authority then that action is unlawful by virtue of Article 6 of that Act (right to a fair trial). The evidence obtained could be excluded in Court under Section 78 Police and Criminal Evidence Act and also risk civil litigation as a consequence.

2. Background

This section serves to explain and highlight the legislation to be considered as well as reaffirming the legality of existing practices.

2.1 Paragraph 2.21 of the Code of Practice states that:

Some surveillance activity does not constitute intrusive or directed surveillance for the purposes of Part II of the 2000 Act and no directed or intrusive surveillance authorisation can be provided for such activity. Such activity includes:

- Covert surveillance by way of an immediate response to events;
- Covert surveillance as part of general observation activities;
- Overt use of CCTV and ANPR systems.

2.2 Paragraph 2.24 further states:

The general observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act, whether covert or

overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people.

2.3 Paragraphs 2.27 – 2.28 gives further specific information:

The use of overt CCTV cameras by public authorities does not normally require an authorisation under the 2000 Act. Members of the public will be aware that such systems are in use, and their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008, issued by the Information Commissioner's Office.

However, where overt CCTV are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV system in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

2.4 The Act is divided into five parts. Part 2 is the relevant part of the Act in relation to the use of CCTV systems by local authorities. It creates a system of authorisations for various types of covert surveillance. The types of activity covered are **'intrusive surveillance'** and **'directed surveillance'.**

3. Surveillance types and definitions

3.1 **Surveillance** – Section 48(2) of the Act states that surveillance includes;

a) Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.

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

c) Surveillance by, or with the assistance of a surveillance device.

3.2 There are significant differences between 'Intrusive' surveillance (which will be a rarity for CCTV operations) and 'Directed' surveillance (which will be the more likely outcome).

3.3 **Covert** – Section 26(9). **Surveillance is Covert if, and only if**, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.

3.4 **Directed surveillance** – Section 26(2). Surveillance is **directed** for the purposes of this Part if it is '**Covert'** but not intrusive and is undertaken:

a) For the purposes of a specific investigation or a specific 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);

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 surveillance.

3.5 **Intrusive surveillance –** This is a highly intrusive form of covert surveillance. It is unlikely that an average CCTV system (public or private) would be capable of acquiring such product without additional technical capability. It is defined as follows:

Section 26(3) - surveillance is intrusive for the purposes of this Part if, and only if, it is 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.

Section 26(5) – surveillance which:

(a) Is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; but

(b) Is carried out without that device being present on the premises or in the vehicle;

Is not intrusive unless the device is such that it 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.

3.6 **Private information** – Section 26(10) – Private information in relation to a person includes any information relating to his/her private or family life.

3.7 Paragraphs 2.4 and 2.5 of the Code of Practice clarify this further:

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/

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. Intrusive Surveillance involving the use of CCTV

4.1 Whilst most CCTV cameras are deemed incapable of providing the level of detail required for Intrusive Surveillance great care should be taken to distinguish between focussing on the exterior of premises and the inside, which **may** be construed as intrusive surveillance.

4.2 CCTV cameras should not be used to look into a private residential property without prior consultation and approval of the local authority and with the correct RIPA 2000 authority in place. Authorisation for this purpose is only likely in very rare circumstances and after all other methods have been tried or considered, as the public do not expect a CCTV system to be utilised in this way.

4.3 Currently, the sustained gathering of images of persons in a car in a car park may be considered unusual, i.e. the use of CCTV to observe drug deals, clearly visible inside a car – but this is not considered to be "intrusive", as the product gained does not consistently provide information of the same quality as might be expected to be obtained from a device actually present in the vehicle. Likewise, as a general principle, a person committing an offence has no expectation of privacy.

5. Directed Surveillance involving the use of CCTV

5.1 This level of covert surveillance is likely to be engaged more by public/private CCTV users when they are requested by "authorised bodies" to operate their cameras in a specific way for a planned purpose or operation where "private information" is likely to be gained.

5.2 If a CCTV user is carrying out normal everyday observations by operating a particular camera to gain the best information, albeit it may not be the most obvious camera to use or the nearest to the incident being observed, that use will not be deemed to be "covert" under the terms of the Act. It is using modern technology to the advantage of the operator and will usually mean focussing on a particular person or location as a result of an immediate set of circumstances. It will only be where CCTV cameras are to be used in a planned, targeted way to gain "private information" that authorised Directed Surveillance **may** be required.

5.3 If users are requested to operate cameras as part of a planned operation, where the subject is unaware that targeted surveillance is, or may be, taking place and "private information"is to be gained which involves systematic surveillance of an individual(s) (whether or not the target of the operation) or where a camera is utilised in a way that it is not usually operated or where members of the public would not expect to be subject of CCTV monitoring by a local authority then a directed surveillance authority **must** be obtained.

6. Consultation between authorities

6.1 Where consultation between officers of the local authority CCTV and Cambridgeshire Constabulary takes place, and advice is given that an authority under the Act is not required, then the officer giving that advice will make a record

of the circumstances in a retrievable form which will be made available for any review at a later date.

6.2 Where a CCTV system is utilised and an authority under the Act is in place, the details of the date and time of the authority being granted, the nature of the offence under investigation, together with the name of the Authorising Officer (A.O.) and authority reference number will be provided in written form to the local authority for their records and any subsequent inspection by the Office of Surveillance Commissioners (hereafter known as the O.S.C.).

6.3 Similarly, where the CCTV system is routinely used within authorised surveillance activity, such information will also be provided to the local authority, in a written form, in respect of any authority review, renewal, or cancellation.

7. Protocols and procedures when dealing with Local Authority CCTV Systems

7.1 The O.S.C. recommends that law enforcement agencies should produce and obtain a written protocol with a local authority if its CCTV system is to be used for directed surveillance. The protocol will include a requirement that the local authority should see, and be provided with a copy of, the authorisation, and only allow its equipment to be used in accordance with it.

7.2 Below is an extract for Operational Officers from the protocol agreed between Cambridgeshire Constabulary and local authority partners.

7.3 **In accordance with the Office of the Surveillance Commissioners Procedures and Guidance (R v Sutherland principle), all officers and staff acting under the authority of a Directed Surveillance should read and sign to say they have read that authority so that they are fully aware of the boundaries and limitations as to what is and is not authorised OR have been suitably briefed by a supervisor who will sign to that effect for that group of officers or staff.**

7.4 In planned operations and where the use of a local authority CCTV as a tactic is planned or likely then such activity should be referred to in the Surveillance application.

7.5 In principle, where a local authority CCTV system is being utilised by Cambridgeshire Constabulary or other law enforcement agencies in its normal format this will not be subject to, or require an authority under the Act.

8. Tasking Agency

8.1 Where the Police use local authority CCTV, or CCTV owned by any other public body and the use of the CCTV requires authorisation under the Act, the question may arise of which agency should authorise the surveillance.

8.2 The Code of Practice (Paragraph 3.16) states, ‘In cases where one agency is acting on behalf of another, it is usual for the tasking agency to obtain or provide authorisation.’

9. Live Surveillance Operations

9.1 Often, without prior knowledge and planning, foot and mobile surveillance operations result in surveillance operatives being required to follow subjects into locations where public CCTV systems are in use, pedestrian shopping areas, sporting venues, transportation systems etc.

9.2 In such unplanned circumstances and where possible, surveillance officers (who will have themselves seen or been briefed as to the content of the authority) should be in a position to quote the operational name to the CCTV staff and give them the details of the Authorising Officer. Further details concerning the date, time, and reference number of the authority will be provided after the event if required by the local authority officer responsible for the CCTV system, or their deputy. Similar details will be provided by the Police if they are acting under an urgent oral authority, granted by the Authorising Officer as permitted under the terms of the Act.

10. Summary

10.1 Directed Surveillance authorities are not required for situations which are an immediate response to events or in circumstances the nature of which are such that it would not be reasonably practicable for a Directed Surveillance authority to be sought. This includes situations which occur in the view of CCTV operatives.

10.2 The Act does not normally apply to overt actions conducted by public authorities.

10.3 However, the Code of Practice, and advice from the Office of The Surveillance Commissioners – Procedures and Guidance 2010, implies that where normally overt CCTV systems are utilised in pre-planned operations, for a specific investigation/targeting a specific individual, whereby there is a likelihood of acquiring private information about that or any other individual then a Directed Surveillance authority **may** be required and that serious consideration should be given by an Authorising Officer as to the privacy of individuals and any breaches or engagement of human rights legislation.

10.4 The principle to be applied is for every individual set of circumstances to be assessed on their own merits, and where there still exists doubt as to the requirement for an authority, advice should be sought from Cambridgeshire Constabulary's Covert Authorities Bureau (C.A.B.) or the dedicated Constabulary Covert Advisors, in consultation with the officer responsible for the local authority CCTV system, or their deputy. Permission to use a system will ultimately fall to the officer within the local authority who is responsible for CCTV, or their deputy, and each decision will be made in line with the policies of each relevant authority.

10.5 The Covert Authorities Bureau can be contacted during office hours on 01480 422343. In cases of urgency the dedicated Covert Advisors or the on call Covert Authorities Bureau Officer can be contacted via the Force Control Room.

11. Protocol

11.1 This Protocol will be reviewed at least annually in consultation with all relevant parties, or in line with changes in legislation, the emergence of relevant case law or national guidance.

11.2 An implementation review will take place within six months of the protocol's commencement through the agreement and signature of all parties.

11.3 This agreement confirms arrangements between Cambridgeshire Constabulary and the Local Authorities within the County for the use of CCTV systems under their control.

11.4 Cambridgeshire Constabulary will not seek the planned use of CCTV systems for directed surveillance operations without the operators / supervisors having details of the date and time of the authority along with the details of the Authorising Officer and authority reference number.

11.5 Any party to this Protocol document can request it to be reviewed at any time.

Signed on behalf of Cambridgeshire Constabulary:

.....

Title:.....

Rank/Position: .....

Date:.....

Signed on behalf of ……..

.....

Title:.....

Rank/Position: .....

Date:.....