MARCH 2002 – REVISED DECEMBER 2003, 2004 2006 AND SEPTEMBER 2009, JUNE 2012 AND AUGUST 2013.

Formatted

Deleted: AND

BOLSOVER DISTRICT COUNCIL'S POLICY AND PROCEDURE ON THE APPLICATION OF PART II OF RIPA

1.0 OBJECTIVE

1.1 To summarise the impact of the Regulation of Investigatory Powers Act 2000, ("RIPA"), particularly Part II (Surveillance and Covert Human Intelligence Sources), on the work of the Council and to formalise procedures already adopted to ensure that the exercise and performance of the powers granted under RIPA are correctly carried out.

2.0 BACKGROUND – RIPA AND HUMAN RIGHTS

2.1 All local authorities undertake functions that require the use of investigatory techniques including surveillance.

2.2 In this Authority these functions would include for example investigations into benefit fraud, planning enforcement, environmental health and housing matters and work by the CAN Rangers.

2.3 On the face of it some types of surveillance may breach an individual's human rights, namely Article 8 of the European Convention of Human Rights and Fundamental Freedoms, Rights to respect for private and family life, which provides that:-

(1) Everyone has the right to respect for his private and family life, his home and is correspondence.

(2) There shall be no interference by a local authority with the exercise of this right except such as in accordance with law and is necessary in a democratic society in the interests of the prevention of disorder or crime.

2.4 The purpose of RIPA is to ensure that local authorities can show that they have considered and balanced the rights of the individual as detailed paragraph 1 of Article 8 against the limitations of the right contained in paragraph 2.

2.5 The Freedoms Act 2012 introduced restrictions to the scope of activities for which the Council can carry out directed surveillance under RIPA. This Policy should be read in the light of those restrictions.

The use of covert surveillance must now meet the "crime threshold". This requires that the offence subject to investigation must be one punishable by a maximum term of at least 6 months imprisonment. The only exception is for investigation of offences related to underage sale of alcohol or tobacco. Directed surveillance can no longer be used for

investigation of low-level offences such as littering, dog control or fly posting.

3.0 THE RIPA AUTHORISATION

3.1 RIPA introduces a system of authorisations, the aim of which is to avoid legal challenge to the use of the evidence obtained using covert surveillance. The Council approved its procedures at Standards Committee on 17th September 2001 and 13th December 2004.

3.2 Following the implementation of the Freedoms Act 2012 the Authorisation process set out in this document is now subject to judicial approval, described in more detail below.

3.3 The central register is kept by the Solicitor to the Council and includes the original of each authorisation, renewal, review and cancellation.

Deleted: 2

Deleted: ¶
¶

3.3 The whole system can and has been inspected by the Office of the Surveillance Commissioner.

4.0 WHAT IS COVERT SURVEILLANCE

4.1 Part II of RIPA refers to covert surveillance. Covert surveillance means surveillance that is carried out in such a way as to ensure that the person under surveillance does not know about the surveillance.

4.2 For the purpose of the Act there are two types of covert surveillance, "directed surveillance" and "intrusive surveillance". The Council is not empowered to undertake intrusive surveillance.

5.0 DIRECTED SURVEILLANCE

5.1 This is covert but not intrusive (and not an immediate response to events) but undertaken for a specific investigation or operation in a way likely to obtain private information about a person. It must be necessary and proportionate to what it seeks to achieve and may be used by the wide range of organisations identified in the legislation. The Council is not empowered to undertake intrusive surveillance.

5.2 An authorisation for directed surveillance may be granted for the purposes of preventing and detecting crime.

5.3 It must be proportionate to what it seeks to achieve.

6.0 INTRUSIVE SURVEILLANCE

6.1 The Council is not empowered to undertake intrusive surveillance.

6.2 Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private

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

6.3 Where surveillance is carried out in relation to anything taking place on any premises or in any vehicle by means of a device without that device being present on the premises or in the vehicle, it is not intrusive unless the device 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. For example information obtained outside premises that provides a limited view and no sound of what is happening inside the premises would not be considered as intrusive surveillance.

6.4 The Council has no statutory powers to interfere with private property. However it is acknowledged that in certain circumstances there may be some degree of trespass which arises in the course of covert surveillance activities, e.g. placing a camera in a hedge to monitor fly-tipping. Where officers believe that covert surveillance may involve some form of trespass the matter should be referred to the Solicitor of the Council as a matter of urgency.

Deleted: .....

7.0 COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

7.1 Provisions in Part II also cover the use of CHIS. The use or conduct of someone who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information and covertly discloses that information is the use of a CHIS. The authorising officer must be satisfied that the authorisation is necessary, that the conduct authorised is proportionate to what is sought to be achieved and that arrangements for the overall management and control of the individual are in force. CHIS may be used by the wide range of organisations identified in the legislation including the Council.

7.2 This does not relate to members of the public who volunteer information which they have received in the course of their normal personal or business life and/or when they have no expectation of reward or advantage.

7.3 The Act regulates the use and conduct of CHIS.

7.4 Use means any action inducing or asking a person to engage as an intelligence source. Conduct is conduct which establishes a personal or other relationship for the purposes of obtaining the information.

7.5 **Currently the Council does not use CHIS**. If an application were received, it would have to be dealt with in accordance with the following rules in addition to those applicable to directed covert surveillance – i.e. for the prevention and detection of crime or preventing disorder, that the Authorising Officer considers that it is proportionate and necessary, details of the nature of the investigation are given, details of any expected collateral inclusion or confidential information are given.

7.6 In addition the authorisation should give a description of the purpose for which the source will be deployed and the nature of what the source will be asked to do.

7.7 Authorisations last for 12 months

7.8 As with other authorisations, there should be regular reviews and renewals applications where necessary. **The authorisation must also be cancelled when it is no longer needed.**

7.9 Anyone intending to apply for a CHIS authorisation needs to supply evidence of a risk assessment as to the safety of the CHIS and that the correct handling arrangements are in place – i.e. that a handler, a controller and a record keeper are in place to deal with the CHIS – currently RIPA (Source Records) Regulations SI 2000/2725.

Deleted: manager

7.10 Records will have to be kept of the dealings with the CHIS in accordance with the relevant regulations.

7.11 If anyone is considering applying for a CHIS authorisation, advice **must** be sought first from the Solicitor to the Council or the Senior Principal Solicitor or the Deputy Monitoring Officer.

8.0 WHEN/HOW CAN WE AUTHORISE

The Authorisation

8.1 The nature of the authorisation required depends upon the nature of the surveillance being undertaken.

8.2 Most surveillance undertaken by Council officers is not covert surveillance at all and does not therefore require authorisation. Other cases will be directed surveillance, not intrusive surveillance. The latter is not undertaken by this Council by law.

8.3 In order to ensure that the provisions of the Act are complied with throughout the organisation, staff are reminded an authorisation for directed surveillance in accordance with the procedures outlined in this RIPA Policy and Procedure must be obtained where directed surveillance is proposed and that whenever an authorisation is granted the authorisation (and any renewals, reviews or cancellations) must be sent to the Solicitor to the Council as soon as possible.

8.4 Before seeking an Authorising officers need to consider:-

8.4.1 Their powers to investigate the matter being investigated, including whether the offence being investigated meets the crime threshold.

8.4.2 Is the proposed action proportionate to the matter being investigated.

I.e. the Authorising Officer must consider whether the use of covert surveillance is proportional to the intrusion on the target and others.

Deleted: I

8.4.3 Could the same information be obtained from a different source.
8.4.4 Is the proposed action in accordance with the relevant Code of Practice (see Appendix C).

8.5 Members of Strategic Alliance Management Team have power to grant authorisations for directed surveillance under RIPA. Please see the attached list of Authorised Officers at Appendix A and forms at Appendix B.

8.6 No Authorising Officer would usually authorise covert surveillance by an officer from their own staff group.

8.7 The legislation requires that an officer giving the authorisation must first satisfy him/herself that the authorisation is necessary on the particular ground and that the surveillance is proportional. This means the Authorising Officer must consider whether the use of covert surveillance is necessary in the particular circumstances. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether serious crime criteria are met. The reasons why it is deemed necessary must be clearly recorded.

8.8 Amongst other things he/she must particularly consider collateral intrusion (interference with the privacy of persons other than the subject(s) of the proposed surveillance) particularly when considering the proportionality of the surveillance. Appendix E includes guidance to Authorising Officers on these issues for when they are considering applications.

8.X In considering proportionality the authorisation should demonstrate how an authorising officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate and is the least intrusive option available.

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

8.X The authorisation should therefore include reference to consideration of:

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,
- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and
- providing evidence of other methods considered and why they were not implemented.

Formatted: Bullets and Numbering

Formatted: Bulleted + Level: 1 + Aligned at: 1.27 cm + Tab after: 1.9 cm + Indent at: 1.9 cm

8.9 Standard forms have been produced and are used by the Council. These forms are designed to ensure that all these issues and others are addressed when officers are seeking an authorisation. Again these

are referred to in Appendix B which has links to the Home Office website.

8.X The key information to be included in the application for authorisation includes:

- Why is the surveillance necessary?
- Who is the surveillance directed against? Including full details of the subject(s).
- Where and When will it take place?
- What surveillance activity/equipment is to be used? Including whether static, foot or vehicular surveillance.
- How is it to be achieved?

Formatted: Font: Not Italic

Formatted: Bulleted + Level: 1 + Aligned at: 1.9 cm + Tab after: 2.54 cm + Indent at: 2.54 cm

Formatted: Font: Not Italic

Formatted: Font: Not Italic

8.10 The forms are as follows:-

Directed Surveillance

Application for Directed Surveillance Authorisation	Form 1
Review of Directed Surveillance Authorisation	Form 2
Renewal of Directed Surveillance Authorisation	Form 3
Cancellation of Directed Surveillance Authorisation	Form 4

Covert Human Intelligence Sources (CHIS)

Application for conduct-use of CHIS Authorisation	Form 5
Review of CHIS	Form 6
Renewal of CHIS Authorisation	Form 7
Cancellation of conduct-use of CHIS Authorisation	Form 8

(Link to the Home Office site that has the up to date version of the above forms are to be found in schedule B below on page 9)

8.11 Authorisations must be given in writing by the Authorising Officer except in urgent cases where they may be given orally but a record of the authorisation must be recorded in writing as soon as is reasonably practicable. This should be done by the person requesting the authorisation but it must then be endorsed by the authorising officer at a later stage. The record should detail the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and authorising officer as a priority. There is then no requirement subsequently to submit a full written application.

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Deleted: ¶

8.12 Authorising officers should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved.

8.13 A written authorisation for directed covert surveillance 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. A CHIS authorisation lasts 12 months.

8.14 Oral authorisations will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

8.15 **Where there is any doubt as to whether or not a surveillance needs authorisation the officer should err on the side of caution and apply for an authorisation.**

8.16 **Intrusive surveillance cannot be undertaken or authorised by officers working for the Council and can only be undertaken with the assistance of the Police in, for example a joint operation.**

8.17 Renewals

The Authorisation may be renewed for a further 3 months at its end by the completion of the appropriate form and further consideration by an Authorising Officer. Consent for renewal will be given in writing. Such a renewal should be made shortly before expiry of the previous authorisation, which will occur at 23:59 on the day preceding the 3 month point. The original Renewal authorisation must be passed to the Solicitor to the Council for inclusion in the Register.

Deleted:

8.18 Authorisations may be reviewed more than once.

8.19 Review

Regular reviews of Authorisations will be undertaken to assess the need for the authorisation. Results of the review should be passed to the Solicitor to the Council for inclusion in the Register.

8.20 It is for the Authorising Officer to decide how frequently a review should be carried out. However reviews should be no less than once a month. The Review period **must** be stated in the Authorisation by the Authorising Officer. Where the surveillance involves a high level of intrusion, or is likely to obtain confidential information, consideration should be given to a shorter review period, particularly as high levels of intrusion can have an impact on proportionality.

8.XX Judicial Approval

Formatted: Underline

Once an authorisation or renewal for directed surveillance has been granted by the authorising officer an application must be made to the Magistrates Court for approval. Only if approval is given can the surveillance take place. NB The application must be made by the public authority that has granted the authorisation.

Home Office Guidance to Local Authorities ("Protection of Freedoms Act 2012 – changes to provisions under the RIPA 2000") sets out the procedures for seeking judicial approval in full.

In summary, the basic procedure once authorisation is granted by the authorising officer will be:

- Contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.
- Provide the Court with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case.
- The original RIPA authorisation or notice should be shown to the Court but will be retained by the local authority. The court may wish to take a copy.
- Provide the Court with a partially completed judicial application/order form.
  NB Although the local authority is required to provide a brief summary of the circumstances of the case on the judicial application form, this must be in addition to the original RIPA authorisation.
- The order section of the form will be completed by the Justice of the Peace and will be the official record of the JP's decision.

In order to approve the authorisation the Court must be satisfied that the reasons for granting the authorisation were reasonable and that the authorising officer was appropriately empowered to do so.

Officers who appear before the Court in making an application must also be properly authorised to do so in accordance with the Council's Constitution. Does this mean we need to change the Constitution?

The local authority will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and the local authority will need to retain a copy of the judicial application/order form after it has been granted. There is no requirement for the JP to consider either cancellations or internal reviews.

Formatted: Bulleted + Level: 1 + Aligned at: 1.9 cm + Tab after: 2.54 cm + Indent at: 2.54 cm

Formatted: Bullets and Numbering

Formatted: Indent: Left: 2.54 cm

Formatted: Bulleted + Level: 1 + Aligned at: 1.9 cm + Tab after: 2.54 cm + Indent at: 2.54 cm

Formatted: Indent: First line: 0 cm

8.21 Cancellation

All Authorisations, even time limited ones, should be cancelled at the earliest opportunity, i.e. as soon as no longer required. The cancellation form must be completed and submitted to the Solicitor to the Council within 28 days of cancellation for inclusion on the Register.

Formatted: Underline

Deleted: need to be cancelled at the end of their use

8.22 **The cancellation must be completed by the Authorising Officer. In the absence of the original Authorising Officer, the cancellation may be given by another Authorising Officer.**

Formatted: Font: Not Bold

8.X When cancelling an authorisation, the authorising officer should:

- Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.
- Record the reason for cancellation.

Formatted: Bullets and Numbering

- Ensure that surveillance equipment has been removed and returned.
- Provide directions for the management of the information gathered.
- Record the value of the surveillance or interference (i.e. whether the objectives were met).

8.X Authorisations may be cancelled orally. When and by whom this was done should be endorsed on the cancellation form when it is completed, and recorded on the Register.

Formatted: Font: Not Bold

8.23 Combined Surveillance

Where surveillance is being undertaken with another agency (eg the Police) only one Authorisation is required for both agencies. A lead in obtaining the authorisation should be taken by the appropriate agency. If this is not the Council, a copy of the other agency's Authorisation should be submitted to the Solicitor to the Council for inclusion on the Register. In all cases of combined surveillance all officers involved should review the Authorisation to familiarise themselves with what has been authorised. Managers must also review the Authorisation to ensure officers do not exceed their level of training.

Deleted: ¶
¶

Formatted: Indent: Left: 0 cm, First line: 0 cm

9.0 THE REGISTER AND ITS MAINTENANCE

9.1 The Solicitor the Council will keep the Register of Authorisations. As confidential information will be contained within the Register it will be kept under lock and key. The purpose of the Register is to ensure that covert surveillance is properly authorised and is carried out by the Council only in accordance with the authorisation, this policy and procedure and the legislation.

Deleted: The Register will include a log of the number and type of authorisations together with all renewals, reviews and cancellations.

9.X The Register will contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- name and job title of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and job title of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled.

Formatted: Bulleted + Level: 1 + Aligned at: 1.9 cm + Tab after: 2.54 cm + Indent at: 2.54 cm

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

9.2 Authorisations will be kept for a period of 3 years from the ending of the Authorisation and will then be destroyed.

9.3 Regular reminders of the need for Authorisations will be given by the Solicitor to the Council through Management Team and by email more generally.

9.4 An Annual report will be made to Standards Committee on the use of Authorisations.

9.5 Access to the Register will be given only on a strict need to know basis.

9.6 The Solicitor to the Council will ensure regular monitoring of compliance with the Council's RIPA Policy and Procedure and the legislation.

9.7 All FBU Managers will ensure their staff are suitably trained and will review training requirements annually.

9.8 Once a year the Solicitor to the Council will arrange a meeting of Authorising Officers and Investigating and Enforcement Officers to review and share information/experience/training.

10.0 OTHER TYPES OF SURVEILLANCE

10.1 The Act also covers other investigatory techniques such as the interception of communications, but as with intrusive surveillance this type of investigatory activity cannot be undertaken or authorised by officers working for the Council.

11.0 CODES OF PRACTICE

11.1 There is a link to these in Appendix C. These are issued by the Home Office. Anyone wishing to undertake covert surveillance or use a CHIS must consider advice in the relevant code.

12.0 THE OFFICE OF THE SURVEILLANCE COMMISSIONER (the "OSC")

12.1 The Act also establishes a Surveillance Commissioner who has a duty to keep under review the exercise and performance of powers and duties under Part II of the Act.

12.2 All those involved in the authorisation process have a duty to provide information to the Surveillance Commissioner at his request. The OSC has written to all public authorities informing them of his responsibilities

to keep under review the exercise and performance of powers and duties under RIPA.

12.3 The OSC has also recently written to all local authorities asking for information to be provided to him.

13.0 FREQUENTLY ASKED QUESTIONS

13.1 A set of FAQs is attached at Appendix D to aid interpretation but officers need to be aware that legislation may change over time and that the advice in this procedure is not meant to be a definitive guide to the law so if you are in any doubt please contact Legal Services.

14.0 OTHER INFORMATION/GUIDANCE

14.1 There are Codes of Practice which officers seeking authorisations and those granting authorisations should familiarise themselves with. These include codes on the use of CHIS's and covert surveillance.

14.2 Enforcement Policies and Procedures must be consistent with the requirements of RIPA.

APPENDIX A

Officers authorised to grant authorisations for directed surveillance under section 28 and Covert Human Intelligence Sources under section 29 of the Regulation of Investigatory Powers Act 2000.

W. Lumley	Chief Executive Officer
S. Tomlinson	Director of Neighbourhoods
B Mason	Director of Corporate Resources
K Hopkinson	Director of Development
P Hackett	Director of Health and Well Being

APPENDIX B

Forms

Directed Surveillance

Application for Directed Surveillance Authorisation	Form 1
Review of Directed Surveillance Authorisation	Form 2
Renewal of Directed Surveillance Authorisation	Form 3
Cancellation of Directed Surveillance Authorisation	Form 4

Covert Human Intelligence Sources (CHIS)

Application for conduct-use of CHIS Authorisation	Form 5
Review of CHIS	Form 6
Renewal of CHIS Authorisation	Form 7
Cancellation of conduct-use of CHIS Authorisation	Form 8

These can all be obtained from the Home Office website on the fllowing link:-

https://www.gov.uk/surveillance-and-counter-terrorism

Deleted: http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/¶

APPENDIX C

CODES OF PRACTICE

The link to Covert Surveillance Code of Practice and Link to Covert Human Intelligence Source (CHIS) Codes of Practice are on the Home Office website. The current link is:-

https://www.gov.uk/surveillance-and-counter-terrorism

Deleted: http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

APPENDIX D

FREQUENTLY ASKED QUESTIONS ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

BACKGROUND

RIPA has the following parts:

PART	CONTENTS	IN FORCE	BDC USE
Part I (Chapter 1)	The interception of communications	02.10.00	No
Part I (Chapter II)	The access and disclosure of communications data		No
Part II	Intrusive surveillance directed surveillance and use and conduct of covert human intelligence sources (known as a 'CHIS'), which would include informants or undercover officers. Intrusive surveillance cannot be undertaken by this Authority.	02.10.00	Yes, except intrusive surveillance
Part III	The investigation of electronic data protected by encryption		No
Part IV	Oversight mechanisms, the establishment of complaints procedures and codes of practice	02.10.00	N/A

GENERAL OVERVIEW

Q1 what does Part II of RIPA cover?

A1 Part II covers the use of surveillance (both intrusive and directed surveillance) and the conduct and use of covert human intelligence sources (agents, informants and undercover officers).

Q2 Can this Council use any of the powers within Part II of RIPA?

A2 **No-one at the Council is able to carry out intrusive surveillance**. However, a designated officer within the Council can authorise the use of directed surveillance and the conduct and use of a covert human intelligence source (CHIS).

Q3 What does directed surveillance and CHIS mean?

A3 The definitions can be found in section 26(2)

(2) ...surveillance is directed for the purpose 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); 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.

And section 26(8), respectively.

(8) For the purposes of this Part a person is a covert human intelligence source if

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling with paragraph (b) or (c);
(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
(c) he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

Q4 Who can authorise directed surveillance and the conduct and use of a CHIS?

A4 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) prescribes the officers who may grant an authorisation. For this Council both directed surveillance and the conduct and use of a CHIS has to be authorised by one of the persons listed in Appendix A.

Deleted: (Prescription of Offices, Ranks and Positions) Order 2000

Deleted: 2000 No. 2417

Q5 What does the authorising officer have to consider?

A5 Whether an authorisation is:

- Necessary on the ground provided in section 28(3) or 29(3) RIPA;
- Proportionate i.e. not a sledgehammer to crack a nut (section 28(2)(b) or section 29(2)(b); and
- Non-discriminatory (Article 14 ECHR)

Formatted: Indent: Left: 1.27 cm

Further guidance on how to reach this decision can be found in paragraph 8.X above.

Q6 How long does an authorisation last for?

A6 The length of an authorisation will vary depending on the type of activity:

A **Directed Surveillance Authorisation** lasts for up to 3 months unless cancelled or renewed. In urgent cases the designated person may orally authorise surveillance for 72 hours, where the person to whom the designated person spoke will compile a written record. **A CHIS authorisation** lasts for a period of 12 months unless cancelled or renewed. **All authorisations must be cancelled when they are no longer necessary or proportionate**

Q7 What forms or records should I use to get the authorisation?

A7 There are standard forms that will require completion, providing evidence to the authorising officer that the criteria and grounds for surveillance have been fulfilled. The forms are to be found in Appendix B via a link to the Home Office website.

Q8 How long do we have to keep authorisation records?

A8 The Codes of Practice require authorisations to be kept for a minimum of 5 years to allow the Chief Surveillance Commissioner to maintain an independent review of the authorisation procedure (see Part IV RIPA).

EXAMPLES / SCENARIOS

Q9 A benefits officer wants to carry out covert surveillance on a person suspected of benefit fraud using photographic equipment to gain further information about his or her activities and associates. What are the implications of RIPA on this activity?

A9 This is 'directed surveillance', which is defined in section 26(2) RIPA because:

- The activity is pre-planned (i.e. it is not in response to immediate events or circumstances (see section 26(2)(c) RIPA);
- It is a covert surveillance operation; and
- It is likely to result in obtaining private information.

The surveillance will require authorisation.

Q10 As an authorised CHIS the officer wants to record meetings with the suspect, using a hidden tape recorder. Does this require any additional authorisation?

A10 No. Once authorisation has been obtained to act as a CHIS the officer will not require any additional authorisation to record those meetings even if he is using a surveillance device (see section 48(3) RIPA).

Deleted: Q10 . The officer, as a result of the above surveillance, wants to establish contact with the suspect. What are the implications of RIPA on this activity?¶
¶
A10 . The officer will become a CHIS, which is defined in section 26(8) RIPA, if he will be establishing a covert relationship with the suspect, for the purpose of obtaining information.¶
¶
. The conduct and use of the CHIS will require authorisation.¶
¶

Deleted: 1

Deleted: A11

Q11 **The officer also wants to use a recording device to record any telephone conversations with the suspect. What are the implications of RIPA on this activity?**

Deleted: Q12

A11 This is directed surveillance as one person consenting to the interception of the communication i.e. the telephone conversation, without the knowledge or consent of the other person (see section 48(4) RIPA). Whether or not an officer is a CHIS, he will need to obtain a directed surveillance authorisation.

Deleted: A12

Q12 **The officer wants to make a hand written note of a telephone conversation, with the suspect, without using a recording device. What are the implications of RIPA on this activity?**

Deleted: Q13

A12 Providing the officer is authorised as a CHIS, no additional authorisation would be required. However, if the officer is not authorised as a CHIS, then consideration would need to be given as to whether the officer is establishing a relationship to covertly obtain information (see section 26(8) RIPA).

Deleted: A13

Q13 **Do I need an authorisation to make a test purchase?**

Deleted: Q14

A13 Where an adult or young person carries out a test purchase, he may be a CHIS and an authorisation for directed covert surveillance **will** be required if technical equipment is worn or the operation is observed by an adult. In all cases a risk assessment must be carried out.

Deleted: 4

Q14 **I want to use a hidden surveillance camera to record a suspect who I have been told is working and claiming benefits. He has a stall in a busy market, close to other traders and I recognise that I may also capture other consumers and traders on the photographs. May I use this surveillance camera and if so what authorisation do I require?**

Deleted: 5

A14 Authority for 'directed surveillance' may be required, if you are likely to obtain private information about the suspect (or any other person). If other members of the public may be photographed it will be important to consider the collateral intrusion issues and whether such surveillance is necessary and proportionate i.e. could other surveillance techniques be used to identify traders and avoid capturing other members of the public on film.

Deleted: 5

Q15 **I have set up a camera viewing the house where the suspect lives, with the intention of observing his movements. In addition to movements at the front door I can see into the lounge. Is this intrusive surveillance?**

Deleted: 6

A15 Although the activities observe an individual in residential premises, it provides a limited view inside the residential premises (see section 26(5) RIPA) and is therefore not intrusive surveillance. Authorisation

Deleted: 6

would be required. In this instance you would be required to obtain directed surveillance authorisation. However, if the camera consistently provides information of the same quality and detail as might be expected from a device actually present on the premises then an intrusive surveillance authorisation would be required and the Council cannot undertake intrusive surveillance.

'Intrusive surveillance' is defined in section 26(3) RIPA as covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

However, local authorities may not lawfully authorise intrusive surveillance activities themselves. If from the start you hope to record activities within the lounge then an intrusive surveillance authorisation is required, providing the operation meets the necessary criteria e.g. for serious crime see section 81(3). However the Council cannot undertake intrusive surveillance and accordingly cannot be authorised.

Q16 I have received a noise complaint and I have asked the complainant to provide a written record detailing the frequency and nature of the noise nuisance e.g. times, source of noise etc. Do I need to obtain any authorisation?

Deleted: 7

A16 This depends on the way that the Council deals with such a complaint. If the local authority receives a complaint and issues a formal letter to the person responsible for the alleged nuisance, which informs them that the Council will be monitoring their premises, any monitoring (as set down in the formal letter) would not be classed as covert surveillance.

Deleted: 7

Q17 To further investigate a noise complaint I have set up a sound level meter (SLM) to record the decibel sound level, with the complainant's consent. Do I need to obtain any authorisation?

Deleted: 8

A17 If the Council sends a formal letter and/or a noise abatement notice, which indicated that monitoring may occur, then by inference this would not be carried out covertly and would not require any authorisation.

Deleted: 8

Q18 To further investigate a noise complaint I have set up two noise recorders in his house to record the noises heard – a sound level meter (SLM) and a DAT recorder (which will record the noises actually heard at their calibration levels). Do I need to obtain any authorisation?

Deleted: 9

A18 If an authority sends a formal letter and/or a noise abatement notice, which indicated that monitoring may occur, then by inference this would not be carried out covertly and would not require any authorisation.

Deleted: 9

If the letter does not indicate that monitoring may occur, and the complainant is asked to assist the local authority to obtain further information (i.e. operate the equipment), this person may be regarded as a CHIS. In this case the type of information obtained during the course of this activity would be within the scope of Article 8 ECHR, as private information may be acquired, and an authorisation should be sought.

Officers should also consider whether any letter and/or noise abatement notice has actually been received and read by the householder, other residents and all other visitors to the property. It is possible that the householder may simply deny receipt of the letter. Any monitoring could therefore be subject to challenges under Article 8 of the European Convention on Human Rights (ECHR) unless authorisation is obtained.

In noise pollution cases particularly, when using equipment to record sound, special care should be taken to ensure that intrusive surveillance is not inadvertently undertaken. This is a danger where the equipment has the facility to pre record or post record an event. If the citing of the equipment and the nature of the equipment mean that, for example, conversations can be recorded this would be intrusive and the equipment should not be used in that way.

Q19 I have set up a camera viewing a shop where the suspect works, with the intention of observing his activities and contacts. I can only see the doorway and entrance to the shop. Do I need to obtain any authorisation?

Deleted: 20

A19 Yes. A directed surveillance authorisation would be required if you are likely to obtain private information.

Deleted: 20

Q20 What is private information?

Deleted: 1

A20 Private information is defined in section 26(10) as any information relating to a person's private or family life.

Deleted: 1

The European Court of Human Rights (ECHR) has said that the term 'private life' must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings. The notion of private life should be taken to include activities of a professional or business nature (*Amann v Switzerland* (2000) 30 ECHR 843).

The Covert Surveillance Code of Practice defines private information as generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

Formatted: Indent: First line: 0 cm

Deleted: ing

Q21 Are overt CCTV surveillance systems regulated by RIPA?

Deleted: Q22

A21 No the provisions of the Act do not generally cover the use of overt CCTV systems. Members of the public are aware that these systems are used overtly for their own protection and to prevent crime.

However, where overt CCTV or ANPR cameras 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 as such surveillance is likely to result in the obtaining of private information.

Also, if the CCTV operators are being investigated, then a directed surveillance authority should be sought.

Deleted: A22

Formatted: Font: Italic

Deleted:

Deleted: However

Formatted: Indent: First line: 0 cm

Q23 I want to place a camera near a public highway, where domestic and business rubbish being tipped, to record individuals committing an offence. The camera may capture other members of the public who park in the lay-by, but are not committing any offences. What do I have to consider and what authorisation will be necessary?

A23 You need to consider whether you are likely to obtain private information as a result of the surveillance. If so, you should consider the necessity and proportionality of obtaining a directed surveillance authorisation, having regard to the issue of collateral intrusion.

APPENDIX E

Guidance for Authorising Officers under RIPA in considering applications for directed surveillance or CHIS

Necessary and Proportionate

1. Is the application truly for covert surveillance?

   E.g. CAN Rangers use a well marked van, the markings explaining that surveillance occurs (not covert) however they can also use the extending mast for the camera on the van and view from a considerable distance in circumstances where the van cannot be seen (covert surveillance).

2. Has the applicant demonstrated that the authorisation for the covert surveillance is necessary and proportionate? If the applicant has not, the authorisation must be refused.

   The applicant may resubmit with further evidence in order to try to establish that the authorisation is necessary and proportionate.

   Necessary

   To demonstrate necessity, you, as Authorising Officer, must believe that the authority is necessary in the circumstances of the particular case. Accordingly, you should ask questions in accordance with

paragraph 8.X above to determine whether or not this is the case and if not, you should refuse the application.

Proportionality

You, as Authorising Officer, must believe that the activities (if authorised) would be proportionate to what evidence is sought in accordance with paragraph 8.X above. You must consider this against the background of the intrusion on the target and others.

This may be established by asking the following questions:-

- Is the intrusion on the target and others balanced by the need for the activity in operational terms?
- Is the activity excessive in the circumstances of the case?
- Can the information be reasonably obtained by other less intrusive means?
- Is the activity arbitrary or unfair?
- Ultimately is the activity necessary?
- Are the proposed activities the least intrusive means of obtaining the evidence.

3. As Authorising Offier, you must not only saitisfy yourself as to it being necessary and proportionate, but you must explain your reasoning.

Reasons should not include:-

- Lack of resources
- Cost saving

as sufficient reason to use more intrusive surveillance methods.

Your potential statement should include an explanation of the following:-

- Balancing the size and scope of the operation against the gravity and extent of the perceived mischief
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others.
- That the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result
- Evidencing what other methods had been considered and why they were not implemented.

4. It is not normally necessary to restrict the duration of the authorisation to specific hours in order to demonstrate proportionality. Operationally this will make compliance more administratively burdensome. **Applicants making applications in this way should be advised to amend the application.**

5. Remember all applications last for 3 months or until cancelled whichever is sooner. Do not accept without amendment applications purporting to be for a shorter period.

6. All authorisations last until midnight on the last day.

Statutory Ground

5. The applicant must demonstrate the applicability of the one ground in section 28(3) (for directed surveillance) or section 29(3) (for CHIS) which applies to the Authority namely:-

   For the purpose of preventing or detecting crime or of preventing disorder;

   If this has not been demonstrated to your satisfaction you should refuse the authorisation.

   Any other grounds quoted should be deleted.

Collateral Intrusion

6. Has the applicant explained what (if any) risk of intrusion there is into the privacy of persons other than those the subject of the surveillance?

   If not the applicant should be required to demonstrate an appraisal of the risk.

   Has the applicant, in cases where there is such a risk, demonstrated how it is proposed that risk is eliminated or minimised?

   If not the applicant should be required to do so before an authorisation is given.

Reviews

7 It is for you, as Authorising Officer, to determine whether the first review should be and how often the authorisation should be reviewed. Do not leave this section blank.

8 Remember that these should be frequent enough to ensure adequate monitoring of the use of the authorisation.

9 The date of the review must be agreed and put in the diary at the authorisation meeting. It should not be left vague and the date must be adhered to.

Renewals

10 As Authorising Officer, you may renew the authorisation for a further period of 3 months. The renewed authorisation will be effective from the date of expiry of the pervious authorisation and can only be considered before the expiry of previous authorisation. The renewal does not have to be granted by the same Authorising Officer, nor is there a restriction on the number of renewals which may be granted – subject to overall reasonableness.

Other Issues

11. Has the conduct/activity to be authorised been adequately described including the nature of the surveillance? So that anyone reading the application is fully aware of what is required?

12. Has the purpose of the activity to be authorised been adequately described? E.g. to establish there is evidence for Court proceedings or that someone is innocent.

13. Have the identities of those to be surveilled been given where possible?

14. Has a description of the information required by the surveillance been given?

15. Have you completed the Authorising Officer's statement as to why directed surveillance is necessary - the who what where when why and how questions? **This box must be completed**. The Authorisation is defective if it is not.

16. Have you completed the Authorising Officer's statement as to why the directed surveillance is proportionate - the who what where when why and how questions? **This box must be completed**. The Authorisation is defective if it is not.

17. It is for the Authorising Officer to specify a period for review of the Authorisation. Please make sure this is included on the form, and arrange an appointment with the applicant on that date.

18. Is this an urgent case? If so please complete/make sure that relevant boxes are completed fully.

CHIS

19. In addition to the above for CHIS make sure that the purpose for which the CHIS is deployed has been adequately described.

20. Also has the applicant adequately described what the CHIS will be tasked to do?

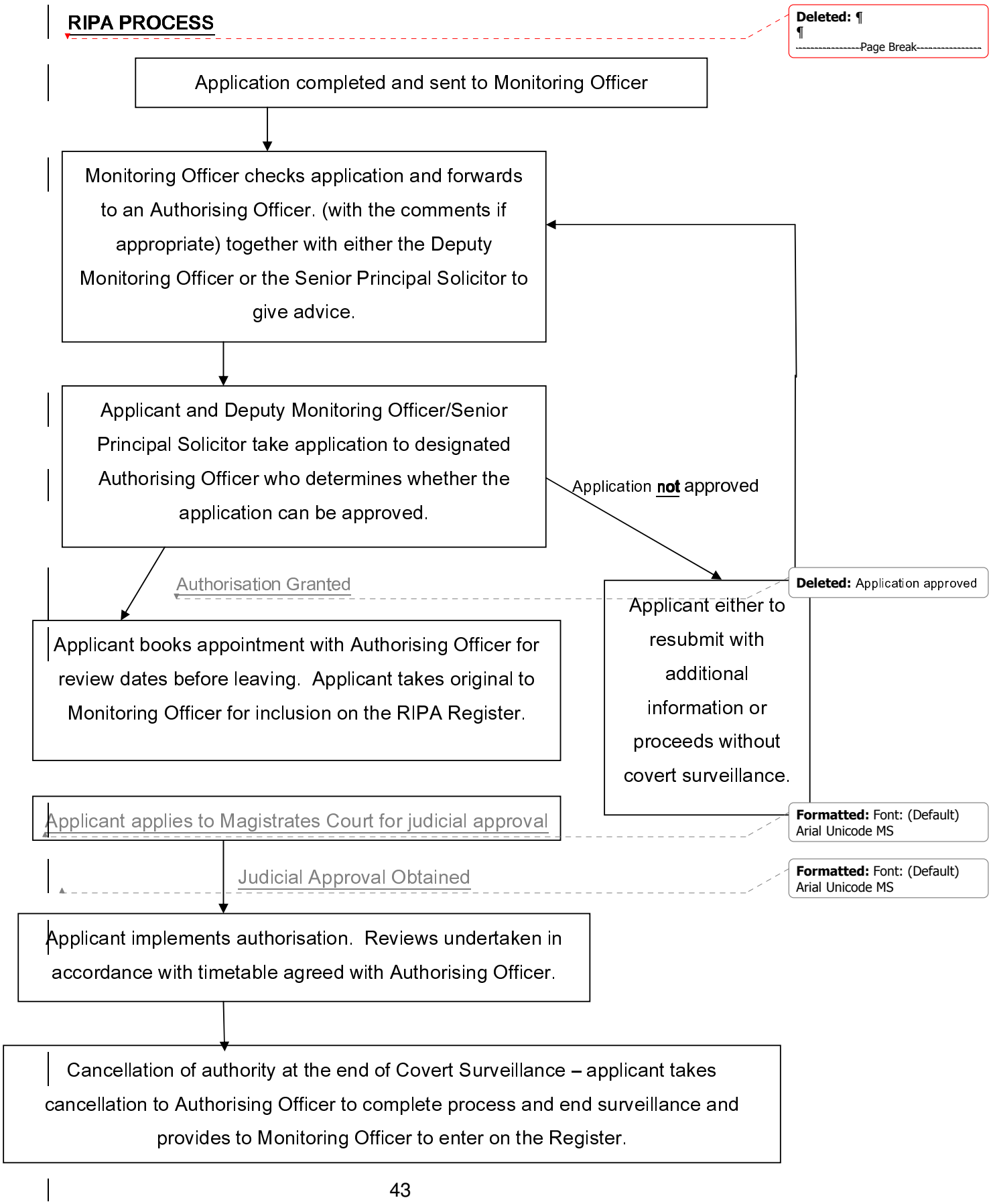
21. Has the risk assessment on the security and welfare of the CHIS been adequately done and explained?

Application

19. The application is for the operation not the individual seeking approval. If an employee leaves having been the applicant, there is no need to cancel and reapply in someone else's name; the operation can continue.

Paperwork

20. The originals of all grants, renewals, reviews or cancellations must be forwarded to the Monitoring Officer in accordance with the flow chart attached.



Deleted: ¶ ¶ ----------Page Break----------

Deleted: Application approved

Formatted: Font: (Default) Arial Unicode MS

Formatted: Font: (Default) Arial Unicode MS

Regulation of Investigatory Powers Act (RIPA)

RIPA provides legality to covert surveillance. Provided authorisations are obtained in accordance with the Act, covert surveillance can be undertaken and the results used in criminal cases in the Courts. Surveillance undertaken covertly without authorisation can result in payment of damages to the person surveilled and to the evidence being disallowed in the Courts.

Introduction

The purpose of this Act is to ensure that any public body – including local authorities - that needs to carry out covert investigation, (which by their very nature may otherwise be in breach of the Human Rights Act 1998) are placed on a legitimate footing and that appropriate controls are put in place to ensure that the activities are properly controlled and monitored.

What is the purpose of RIPA?

The provisions of RIPA are designed to regulate any act of covert investigation or surveillance carried out by a local authority in relation to the purpose of preventing or detecting crime or preventing disorder.

The Human Rights Act introduced a remedy for persons claiming that their privacy had been breached. The effect of Part II of RIPA is to provide protection to the local authority itself **and to the individual officer** against any such claim, provided it is possible to demonstrate full compliance with the procedures prescribed by RIPA. For this Council, those procedures are contained within the RIPA Policy and Procedure which is on ERIC.

If an investigation is carried out in accordance with the Council's RIPA procedures, then any breach of the subject's privacy rights would not be actionable as a civil claim. In addition, in criminal proceedings arising from the investigation, the evidence gathered will not be challengeable under Section 78 of the Police & Criminal Evidence Act 1996, on the ground that it is a breach of privacy rights.

It is therefore crucial that all investigating officers adhere to the requirements of RIPA.

This means that all enforcement officers (and anyone else who may undertake surveillance) should make themselves familiar with the Council's RIPA Policy and Procedure which is on ERIC. You should also ensure that you consider whether what you are seeking to do is such that you should make an application under RIPA.

Advice is always available from the Solicitor to the Council and Legal Services.

Training – this is currently being arranged for all Authorising Officers. There will be a limited number of additional places for those who seek authorisation under the RIPA procedures. This training will be in December and your managers will be told of the available spaces on a first come first serve basis. Regular training is essential for **all** using RIPA.