ITEM NO. F4a

Subject: Regulation of Investigatory Powers Act – Revised Codes of Practice		**Status:**	For Publication
Report to:	Policy Overview and Scrutiny Council	**Date:**	8th March 2011 23rd March 2011
Report of:	Director of Business		
Portfolio Holder:	Finance and Resources		
Key Decision: No			
Forward Plan [X]	General Exception [ ]	Special Urgency [ ]	

1. PURPOSE OF REPORT

1.1 In April 2010 the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 came into force and the Home Office has issued two revised Codes of Practice. These require the Council to take certain action to implement new responsibilities in respect of its activities authorised under the Regulation of Investigatory Powers Act 2000 ("RIPA"). The revised Codes of Practice are titled, "Covert Surveillance and Property Interference" and "Covert Human Intelligence Sources".

2. CORPORATE PRIORITIES

2.1 The matters discussed in this report impact directly on the following corporate priorities:-

A clean and green Rossendale – creating a better environment for all.

A healthy and successful Rossendale – supporting vibrant communities and a strong economy.

Responsive and value for money local services – responding to and meeting the different needs of customers and improving the cost effectiveness of services.

3. RISK ASSESSMENT IMPLICATIONS

3.1 All the issues raised and the recommendation(s) in this report involve risk considerations as set out below:

By not taking the actions required as a result of the Home Office's revised codes of practice, the Council would run the risk of criticism, complaint, having evidence ruled in admissible in court proceedings, claims for unlawful interference with individuals human rights, costs and damages.

4. BACKGROUND AND OPTIONS

4.1 The RIPA, regulates the use of directed covert surveillance, including the use of a covert human intelligence source, (CHIS), i.e. undercover officers seeking to gain the confidence of offenders. RIPA creates a statutory authorisation scheme for the lawful undertaking of such activities.

4.2 In summary, the RIPA requires that when the Council undertakes directed surveillance or uses CHIS for the purpose of the prevention or detection of crime, these activities must be authorised by an authorising officer.

4.3 Directed covert surveillance or CHIS which has been duly authorised under RIPA by an appropriate authorising officer, will be justified as a lawful interference with an individual's right to respect for private family life.

4.4 RIPA activity conducted by local authorities is subject to inspection by the Office of the Surveillance Commissioner and the Council has recently been notified that its next inspection will be in May 2011.

4.5 Rossendale Borough Council is not a frequent user of RIPA. The number of authorisations for the previous three years is as follows:-

For the year ending 31st March 2009 – 3 directed surveillance, 0 CHIS.
For the year ending 31st March 2010 – 5 directed surveillance, 0 CHIS.
For the year ending 31st March 2011 – 0 directed surveillance, 0 CHIS.

4.6 Some covert surveillance undertaken by certain local authorities has been the subject of adverse media coverage, which led to calls for a change in the rules governing such activities. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and the two revised Codes of Practice create new duties and responsibilities. As a result, it is necessary for us to review our practices and procedures under RIPA.

4.7 The revised Code of Practice for Covert Surveillance and Property Interference provides:

"It is considered good practice that within every relevant public authority, a senior responsible officer should be responsible for:

- the integrity of the process in place within the public authority to authorise directed surveillance.
- compliance with Part II of the 2000 Act [surveillance and covert human intelligence sources].
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementations of any post inspection action plans recommended or approved by a Commissioner"

The revised code goes on to say that:

"Within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all relevant officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring concerns are addressed."

4.8 Currently, the Director of Business is responsible for the day to day management of the Council's functions in relation to RIPA. In view of the above, it is recommended that the Director of Business be appointed Senior Responsible Officer for the purposes of RIPA.

4.9 The revised Code of Practice considers the following to be good practice:

"… elected members of a local authority should review the authority's use of the 2000 Act and set policy at least once a year. They should also consider internal reports on use of the 2000 Act on a least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not however, be involved in making decisions on specific authorisations."

4.10 Currently, RIPA is not reviewed by the Council's elected members. In order to comply with the Code, it is recommended that Policy Overview & Scrutiny consider RIPA authorisations on a quarterly basis and that Cabinet review RIPA authorisations and the Council's RIPA policy annually.

4.11 The level/rank of officer able to authorise covert surveillance has also been altered from, "Assistant Chief Officer, Service Manager or equivalent, or any more senior officer", to "Director, Head of Service, Service Manager or equivalent". All officers listed within the Council's RIPA policy meet this definition.

4.12 It should be noted that there are currently plans to ban the use of powers in RIPA by councils, unless signed off by a Magistrate and required for stopping serious crime. The Freedom Bill is expected to be laid before Parliament in mid February 2011 which will introduce the Magistrates' Courts approval process.

COMMENTS FROM STATUTORY OFFICERS:

5. SECTION 151 OFFICER

5.1 Adoption of the recommendations will assist in safeguarding the Council to any financial exposure.

6. MONITORING OFFICER

6.1 The legal issues relating to this matter are referred to in the report, policy and appendices.

7. HEAD OF PEOPLE AND POLICY (ON BEHALF OF THE HEAD OF PAID SERVICE)

7.1 No HR Implications.

8. CONCLUSION

8.1 The recommendations contained in this report are necessary to meet the requirements of revised Home Office Codes of Practice concerning covert surveillance undertaken under RIPA.

9. RECOMMENDATION(S)

9.1 Members are asked to agree that:-

a. The changes to the Council's Policy Statement attached at Appendix A be approved and be adopted with immediate effect; and

b. The Director of Business be appointed as the "Senior Responsible Officer" for the purposes of RIPA (and the Constitution be updated to reflect this); and

c. Cabinet be authorised to review the Council's RIPA Policy and the use of RIPA annually and report to the Portfolio Holder, should they be of the opinion that it is not fit for purpose; and

d. Performance Overview and Scrutiny Committee be authorised to consider the Council's use of RIPA every quarter to ensure that it is being used consistently with the Council's Policy.

e. All future minor amendments to the Policy to be delegated to the Director of Business in consultation with the Portfolio Holder.

10. CONSULTATION CARRIED OUT

10.1 None.

11. COMMUNITY IMPACT ASSESSMENT

Is a Community Impact Assessment required	No
Is a Community Impact Assessment attached	No

12. BIODIVIERSITY IMPACT ASSESSMENT

Is a Biodiversity Impact Assessment required	No
Is a Biodiversity Impact Assessment attached	No

Contact Officer	
Name	Sian Roxborough
Position	Head of Legal Services
Service / Team	Legal Services
Telephone	01706 252496
Email address	sianroxborough@rossendalebc.gov.uk

Background Papers	
Document	Place of Inspection
Appendix A – Updated RIPA Policy.	Attached.
Appendix B - Summary of Main Changes.	Attached.
Appendix C - Home Office Revised Code of Practice - "Covert Surveillance and Property Interference"	Web site: http://www.rossendale.gov.uk/downloads/Item_D2._App_D_-_Code_of_Practice_-_Covert_Surveillance.pdf
Appendix D - Home Office Revised Code of Practice - "Covert Human Intelligence Sources"	Website: http://www.rossendale.gov.uk/downloads/Item_D2._App_C_-_Code_of_Practice_-_Human_Intel.pdf

SUMMARY OF AMENDMENTS TO THE RIPA POLICY

TO BE APPROVED BY FULL COUNCIL ON 23RD MARCH 2011

New paragraph 9:-

INTERNAL REVIEWS

This policy and the Council's use of RIPA shall be reviewed by Cabinet annually.

Internal reports on the Council's use of RIPA shall be considered by Performance Overview and Scrutiny on a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

New paragraph 1.2:-

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 provides that a Director, Head of Service, Service Manager or equivalent may authorise surveillance.

New paragraph 1.3:-

1.3 Senior Responsible Officer

The Director of Business is the Council's Senior Responsible Officer for the purposes of RIPA and shall be responsible for:

- the integrity of the process in place within the Council to authorise directed surveillance.
- compliance with Part II of the 2000 Act.
- engagement with the Commissioners and inspectors when they conduct their inspections.
- Where necessary, overseeing the implementations of any post inspection action plans recommended or approved by a Commissioner.
- ensuring that all relevant officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners.
- Where an inspection report highlights concerns about the standards of authorising officers, the Senior Responsible Officer will be responsible for ensuring concerns are addressed.

Update of job titles on the Authorised Officer List and throughout the Policy as a whole.

CODE OF PRACTICE FOR CARRYING OUT SURVEILLANCE UNDER

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

This document sets out the requirements for gaining authorisation under RIPA, the persons able to grant authorisation, circumstances when authorisation will be required and the storage and maintenance of records of authorisation and the forms which Rossendale Borough Council use.

Stuart Sugarman
Director of Business

Amended and approved by Council on 23rd March 2011

CONTENTS

1.1 **INTRODUCTION**

The Regulation of Investigatory Powers Act 2000 (the 2000 Act) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

Rossendale Borough Council is therefore included within the 2000 Act framework with regard to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources.

The purpose of this guidance is to:

explain the scope of the 2000 Act and the circumstances where it applies provide guidance on the authorisation procedures to be followed.

The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and each Department should hold copies to which staff can refer.

PURPOSE OF RIPA 2000

1.2 On the 2nd October 2000 the Human Rights Act 1998 (HRA) came into full force, making it unlawful for a local authority to breach any article of the European Convention on Human Rights (ECHR).

Article 8 of the ECHR provides :

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

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of National Security/Public Safety/The economic wellbeing of the country/The prevention of disorder or detection of crime/The protection of health or morals/The protection of the rights and freedom of others. (NB. Local Authorities may only use RIPA surveillance for the purpose of the prevention of disorder of detection of crime). Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003, No. 3171.

Definitions

"Detecting Crime" section 81(5) provides for the purposes of this Act detecting crime shall be taken to include:-

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

(b) the apprehension of the person by whom any crime was committed.

"Preventing Disorder" e.g. Anti Social Behaviour

Those who undertake Covert Surveillance on behalf of a Public Authority (whether employees or agents) will breach a person's Human Rights unless the surveillance is authorised in accordance with the LAW and NECESSARY and PROPORTIONATE for the purpose of prevention or detection of crime and disorder.

RIPA came into force on the 1st August 2002. This Code of Practice has been specifically drafted for Rossendale Borough Council.

This Code of Practice only covers Covert Surveillance any Overt Surveillance falls outside RIPA.

In summary the 2000 Act requires that when the Council undertakes "directed surveillance" or uses a "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied.

Authorisation for both types of surveillance may be granted by an authorising officer where it is believed that the authorisation is necessary and the authorised surveillance is proportionate to that which is sought to be achieved :

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 which came into force on the 5th January 2004 places restrictions on the grounds for authorisations under Section 28 (3) and 29 (3) of RIPA to the following :

"For the purpose of preventing and detecting crime or preventing disorder".

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 provides that a Director, Head of Service, Service Manager or equivalent may authorise surveillance.

1.3 Senior Responsible Officer

The Director of Business is the Council's Senior Responsible Officer for the purposes of RIPA and shall be responsible for:

- the integrity of the process in place within the Council to authorise directed surveillance.
- compliance with Part II of the 2000 Act.
- engagement with the Commissioners and inspectors when they conduct their inspections.
- Where necessary, overseeing the implementations of any post inspection action plans recommended or approved by a Commissioner.

- ensuring that all relevant officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners.
- Where an inspection report highlights concerns about the standards of authorising officers, the Senior Responsible Officer will be responsible for ensuring concerns are addressed.

1.4 General Provisions about Authorisations

Surveillance must only be authorised where it is believed that the surveillance is necessary for the prevention and detection of crime or preventing disorder e.g. there is no other reasonable available overt method of finding out the desired information.

Proportionate the method of surveillance proposed is not excessive by relation to the seriousness of the mischief to be investigated : no less invasive method of investigation is available and any collateral intrusion is minimised.

The following positions are authorising officers for the purposes of the Regulation of Investigatory Powers Act 2000.

Chief Executive, Director of Business, Director of Customers and Communities, Head of Legal and Democratic Services, Head of Finance and Property, Head of Customer Services and ICT, Communities Manager, Head of Health, Housing and Regeneration

Amendments to this list are to be agreed with the Director of Business. Amendments are to be recorded on the central legal file.

Formal written authorisation is required to be an authorised officer and this will be reviewed on a case by case basis.

Authorisation under the 2000 Act gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8(1) of the European Convention on Human Rights which is now enshrined in English law through the Human Rights Act 1998.

This is because the interference with the private life of citizens will be “in accordance with the law” and lawful for all purposes. Provided activities undertaken are also “reasonable and proportionate”. The Covert Surveillance and any evidence thus obtained will be immune to challenge in criminal or civil Court proceedings, in cases before Tribunals and conversely if the Council is challenged either by an action for damages under S7 of the Human Rights Act or by way of complaint to the Local Ombudsman or to the Investigatory Powers Tribunal.

It should be noted that the Council cannot authorise “Intrusive Surveillance”.

1.5 Authorising Officers and investigators within the Council are to note that the 2000 Act **does not extend powers to conduct Intrusive Surveillance.** Investigators should familiarise themselves with the provisions of Sections 4 and 5 of the Code of Practice on Directed Surveillance to ensure a good understanding of the limitation of powers within the 2000 Act.

1.6 Deciding when authorisation is required involves making a judgment. Paragraph 2.4 explains this process in detail. If you are in any doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Director of Business. However, it is always safer to get authorisation.

1.7 Surveillance of Council employees/members

Only the Chief Executive and Director of Business have the power to authorise Directed Surveillance the use of Covert Human Intelligence sources concerning any Council member or employee.

2. DIRECTED SURVEILLANCE

2.1 What is meant by Surveillance?

"Surveillance" includes:

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
(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.

2.2 When is surveillance directed?

Surveillance is "Directed" for the purposes of the 2000 Act 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 is 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 to be sought for the carrying out of the surveillance.

2.3 Surveillance becomes intrusive if the covert surveillance:

(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; or

(c) 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 is carried out without that device being present on the premises or in the vehicle, where 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.

2.4 Before any officer of the Council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within the 2000 Act. In order to do this the following key questions need to be asked.

2.4.1 **Is the surveillance covert?**

Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place.

If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not apply.

2.4.2 **Is it for the purposes of a specific investigation or a specific operation?**

For example, are CCTV cameras which are readily visible to anyone walking around a Council car park covered?

The answer is not if their usage is to monitor the general activities of what is happening in the car park. If that usage, however, changes, the 2000 Act may apply.

For example, if the CCTV cameras are targeting a particular known individual, and are being used in monitoring his activities, that has turned into a specific operation which will require authorisation.

2.4.3 **Is it in such a manner that is likely to result in the obtaining of private information about a person?**

"Private information" is any information relating to a person's private or family life.

It is helpful to have regard to the judgement in the case of [Amann v Switzerland Feb 2000] in relation to Article 8 it said "respect for private life comprises the right to establish and develop relationships with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature"

For example, if part of an investigation is to observe a member of staff's home to determine their comings and goings then that would be covered.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework.

If in doubt, it is safer to get authorisation.

2.4.4 **Otherwise than by way of an immediate response to event or circumstances where it is not reasonably practicable to get authorisation.**

The Home Office gives the example of an immediate response to something happening during the course of an observer's work, which is unforeseeable.

However, if as a result of an immediate response, a specific investigation subsequently takes place that brings it within the 2000 Act framework.

2.4.5 **Is the Surveillance Intrusive?**

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and requires the presence of the person gathering the evidence on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as it if were.

Commercial premises and vehicles are therefore excluded from intrusive surveillance. The Council is not authorised to carry out intrusive surveillance.

3. COVERT USE OF HUMAN INTELLIGENCE SOURCE (CHIS)

Although the provisions for a CHIS are not explicitly related to "Private Information" any CHIS operation is certain to infringe privacy rights.

In authorising any CHIS the authorising officer must be satisfied as to the tests of necessity and proportionality of the surveillance and that the matters outlined in paragraph 3.4 have been satisfied.

Use of Juvenile or a Vulnerable person on a CHIS

If it is intended to use a juvenile or a vulnerable person as a source advice should be sought from the Director of Business.

3.1 A person is a Covert Human Intelligence source if:

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c).

(b) he covertly uses such a relationship to obtain information or 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.

3.2 A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

3.3 The above clearly covers the use of professional witnesses to obtain information and evidence.

Additional Requirements for authorisation of Covert Human Intelligence Sources only.

3.4 CHIS may only be authorised if the following additional arrangements are in place

- There is an employee of the Council with day to day responsibility for dealing with the source and for the sources security and welfare.
- There is a Senior Officer who has general oversight of the use made of the source.
- An Officer will be responsible for maintaining a record of the use made of the source.
- These records will contain any matters specified by the Secretary of State in the Regulation of Investigatory Powers (Source Records) Regulations 2000.
- That records disclosing the identity of the source will not be made available to other except on a need to know basis.

Advice should be sought as outlined in paragraph 1.5 on the above.

If in doubt it is safer to obtain authorisation.

4. AUTHORISATIONS, RENEWALS AND DURATION

4.1. The Conditions for Authorisation

4.1.1. Directed Surveillance

4.1.1.1. For directed surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

(a) that an authorisation is necessary (on the grounds detailed below) and

(b) the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

4.1.1.2. An authorisation is necessary if it is:

(a) for the purpose of preventing or detecting crime or of preventing disorder;

4.1.1.3. **The onus is therefore on the person authorising such surveillance to satisfy themselves it is:**

(a) necessary for one of the grounds stated above and;

(b) proportionate to its aim.

4.1.1.4. In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. The forms in the Appendix are to be completed where relevant.

4.1.2. **Covert use of Human Intelligence Sources**

4.1.2.1. The same principles as Directed Surveillance apply. (see paragraph 4.1.1.2 above).

4.1.2.2. The conduct so authorised is any conduct that:

(a) is comprised in any such activities involving the use of a covert human intelligence source, as are specified or described in the authorisation;

(b) relates to the person who is specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and

(c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

4.1.2.3. In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. As such, the forms attached are to be completed where relevant.

It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against that is authorised.

4.2. **Requirements of the 2000 Act**

4.2.1. For urgent grants or renewal, oral authorisations are acceptable. These authorisations will be given by the Authorising Officer or the Officer entitled to act in urgent cases. In such cases a statement that the Authorising Officer has expressly authorised the action should be recorded in writing by the applicant as soon as is reasonably practicable. In all other cases, authorisations must be in writing. In the Appendix to this guidance are standard forms, which must be used. Officers must direct their mind to the circumstances of the individual case with which they are dealing, when completing the form.

4.2.2. Although it is possible to combine two authorisations in one form the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a source.

4.2.3. Authorisations lapse, if not renewed:

- within 72 hours if either granted or renewed orally, (or by a person whose authorisation was confirmed to urgent cases) beginning with the time of the last grant or renewal, or

- in Directed Surveillance cases 3 months from the date of their grant or latest renewal.

- in CHIS cases 12 months from the date of their grant or latest renewal.

4.2.4. Any person entitled to grant a new authorisation can renew an existing authorisation in the same terms at any time before it ceases to have effect.

But, for the conduct of a covert human intelligence source an Authorised Officer should not renew unless a review has been carried out and that person has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

4.2.5. The benefits of obtaining an authorisation are described in paragraph 7 below.

Reviews

Regular reviews of authorisation should be undertaken to assess the need for surveillance to continue. The results of any review should be kept on the central register in Legal and Democratic Services. There will be a greater requirement to review authorisation where the surveillance provider accepts confidential information or collateral intrusion.

4.2.6. **Factors to consider**

Any person giving an authorisation should first satisfy him/herself that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve.

4.2.7. Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

4.2.8. **An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. The authorising officer will take this into account, particularly when considering the proportionality of the surveillance.**

4.2.9. Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

4.2.10. Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

Home Surveillance

4.2.11. The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance at his/her home, or where there are special sensitivities. Article 8 of the Human Rights Act states that everyone has the right to respect for his private and family life, his home and his correspondence.

Spiritual Counselling

4.2.12. No operations should be undertaken in circumstances where investigators believe that surveillance will lead to them to intrude on spiritual counselling between a Minister and a member of his/her faith. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.

Confidential material

4.2.13. The 2000 Act does not provide any special protection for "confidential material" (see the definitions in Appendix 1). Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under this code.

In cases where the likely consequence of the conduct of a source *or as a consequence of directed surveillance* would be for any person to acquire knowledge of confidential material, the deployment of the source *or authorisation of directed surveillance* should be subject to special authorisation.

Advice should be sought from the Director of Business regarding any surveillance likely to involve obtaining Confidential Information.

4.2.14. In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises. *Authorisation in these cases must be sought from the Chief Executive or in his absence a Chief Officer.*

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

- Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Director of Business before further dissemination takes place;
- Confidential material should not be retained or copied unless it is necessary for a specified purpose;
- Confidential material should be disseminated only where an appropriate Officer (having sought advice from the Director of Business) is satisfied that it is necessary for a specific purpose;
- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.
- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

Combined authorisations

4.2.16. A single authorisation may combine two or more different authorisations under the 2000 Act. Combined authorisations must not include intrusive surveillance activity.

4.2.17 In cases of joint working, for example, with other agencies on the same operation, authority for directed surveillance by the relevant authorising officer must be obtained. Authority cannot be granted by the authorising officer of another body for the actions of Council staff and vice versa.

Handling and disclosure of product

4.2.18 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 4.2.15 above.

4.2.19 Authorising Officers are responsible for ensuring that authorisations *including covert human intelligence services* undergo monthly reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

4.2.20 Authorising Officers must ensure that the original authorisations are sent to the Director of Business as described in paragraph 5 below*, so that a central record of all authorisations can be maintained.*

The central record will contain the following information

- *the type of authorisation*
- *the date of authorisation was given*
- *name and rank/grade of the authorising officer*
- *the unique reference number 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 is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer*
- *whether the investigation or operation is likely to result in obtaining confidential information*
- *the date the authorisation was cancelled*

4.2.21 **The original applications for directed surveillance *and CHIS authorisation* will be retained by the Director of Business for a period of 5 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.**

4.2.22 Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

4.2.23 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the Council, of any material obtained by means of covert surveillance and, other than in pursuance of the

grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

4.3 The use of Covert Human Intelligence Sources

4.3.1 Nothing in the 2000 Act prevents material obtained by an employee acting as a source being used as evidence in Court proceedings.

4.3.2 **The Authorising Officer must consider the safety and welfare of an employee/other person acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration from the start for the safety and welfare of the source, even after cancellation of the authorisation, should also be considered.**

4.3.3 The Authorising Officer must believe that the authorised use of the source is proportionate to what it seeks to achieve. Accurate and proper records should be kept about the source and tasks undertaken.

4.3.4 Before authorising the use of a source, the authorising officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

4.3.5 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, "confidential material" is likely to be obtained.

4.3.6 Additionally, the Authorising Officer should make an assessment of any risk to a source in carrying out the proposed authorisation.

5. CENTRAL REGISTER OF AUTHORISATIONS

5.1. The 2000 Act requires a central register of all authorisations to be maintained. The Director of Business maintains this register.

5.2. Whenever an authorisation is granted the Authorising Officer must arrange for the original form details to be forwarded to the Director of Business.

5.3. It is each department's responsibility to securely retain a copy of all authorisations within their departments. Authorisation should only be held for as long as it is necessary and at the appropriate time the records held by the department should be disposed of as confidential waste in an appropriate manner (e.g. shredded).

6. CODES OF PRACTICE

There are Home Office codes of practice that expand on this guidance and copies are held by the Director of Business for access by the public.

The codes do not have the force of statue but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, "if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under the 2000 Act, or to one of the commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account".

Staff should refer to the Home Office Codes of Conduct for supplementary guidance, copies are attached to this guidance.

7. BENEFITS OF OBTAINING AUTHORISATION UNDER THE 2000 ACT

7.1 Authorisation of surveillance and human intelligence sources

The 2000 Act states that

- if authorisation confers entitlement to engage in a certain conduct and
- the conduct is in accordance with the authorisation, then
- it shall be "lawful for all purposes"

However, the corollary is not true – i.e. if you do not obtain the 2000 Act authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits.

7.2 The 2000 Act states that a person shall not be subject to any civil liability in relation to any conduct of his which –

(a) is incidental to any conduct that is lawful by virtue authorisation; and
(b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

8. SCRUTINY AND TRIBUNAL

8.1 To effectively "police" the 2000 Act, Commissioners regulate conduct carried out under thereunder. The Chief Surveillance Commissioner will keep under review, among others, the exercise and performance by the persons on whom are conferred or imposed, the powers and duties under the Act. This includes authorising directed surveillance and the use of covert human intelligence sources.

8.2 A tribunal has been established to consider and determine complaints made under the 2000 Act if it is the appropriate forum. Complaints can be made by persons aggrieved by conduct e.g. Directed Surveillance. The forum hears

application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if:

- A Council officer has granted any authorisation under the 2000 Act.
- Council employees have engaged in any conduct as a result of such authorisation.
- A disclosure notice requirement is given.

9. INTERNAL REVIEWS

This policy and the Council's use of RIPA shall be reviewed by Cabinet annually.

Internal reports on the Council's use of RIPA shall be considered by Performance Overview and Scrutiny on a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

10. COUNCIL POLICY.

10.1 This Policy applies to all Council Service areas. Individual RIPA Policies for Service Areas are not permitted.

DEFINITIONS UNDER THE ACT

Appendix 1 – Application for Authorisation to carry out Directed Surveillance

Appendix 2 – Review of Directed Surveillance Authorisation

Appendix 3 – Renewal of Directed Surveillance Authorisation

Appendix 4 – Cancellation of Directed Surveillance Authorisation

Appendix 5 – Application for Authorisation of the use of CHIS

Appendix 6 – Review of CHIS

Appendix 7 – Renewal of CHIS

Appendix 8 – Cancellation of CHIS

Appendix 9 – Sample Forms

Appendix 10 – Surveillance Risk Assessment Pro Forma

Appendix 11 – Change of Circumstances

Appendix 12 – Surveillance Control Matrix

DEFINITIONS FROM THE 2000 ACT

- "**2000 Act"** means the Regulation of Investigatory Powers Act 2000.
- "**Confidential Material"** consists of:

  (a) matters subject to legal privilege;
  (b) confidential personal information; or
  (c) confidential journalistic material

- **"Matters subject to legal privilege"** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below).

- **"Confidential Personal Information"** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  (a) to his/her physical or mental health; or
  (b) to spiritual counselling or other assistance given or to be given, and

  which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office (see Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

  (c) it is held subject to an express or implied undertaking to hold it in confidence; or
  (d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- "**Confidential Journalistic Material"** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

- **"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;

- **"Authorising Officer"** means a person designated for the purposes of the 2000 Act to grant authorisations for directed surveillance. (SI 2003 No 3171)

- **NOTE A.** Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending

to hold or use them for a criminal purpose; privilege is not lost if a professional legal advisor is property advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.

NOTE B. Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.