Appendix 1

Regulation of Investigatory Powers Act 2000 Policy

LONDON BOROUGH OF EALING

REGULATION OF INVESTIGATORY POWERS ACT 2000

CORPORATE POLICY DOCUMENT ON DIRECTED SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

Revised September 2015

Contents

Introduction

The purpose of this policy is to explain the scope of Regulation of Investigatory Powers Act 2000 (RIPA) and the circumstances where it applies to the Council. In particular it provides guidance on the authorisation procedures to be followed in the event that you need to undertake surveillance, setting it into context so that its importance may be appreciated. The scope of RIPA in relation to Accessing of Communications Data under Part 1, Chapter 2 of the Legislation is set out in a separate policy.

In preparing this policy the Council has followed the Revised Codes of Practice (April 2010) (as amended) produced by the Home Office and all the recent legislative amendments. It has also gained significantly from the advice and support provided by the Office of Surveillance Commissioners.

The subject covered by this policy is complicated but of major importance. It is likely that you may have questions which will not be answered explicitly by the content of this document and these should be referred to the Director of Legal and Democratic Services for assistance.

If having read this document you are unclear about any aspect of the process, seek the advice of the Director of Legal and Democratic Services, an Authorising Officer or RIPA Legal Advisor.

However, if having taken advice doubt exists as to whether the circumstances require an authorisation for consideration under this legislation, you should submit an application form to be authorised. This will demonstrate to any examining body that the Council has taken its responsibilities seriously with regards to the protection of a person's privacy against the need for the activity to take place in operational terms. If you do not secure an authorisation it leaves any evidence gathered open to challenge under section 78 of the Police and Criminal Evidence Act as well as challenges for breach of privacy against the Council.

To assist with oversight of the Council's RIPA processes it has appointed Helen Harris, Director of Legal and Democratic Services as the Senior Responsible Officer whose responsibilities are:

- the integrity of the process in place within the Council to authorise directed surveillance
- compliance with the legislation and Codes of Practice.
- engagement with the Commissioners and Inspectors when they conduct their inspections
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.
- ensuring that all *authorising 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 the concerns are addressed.

It will also be the SRO's responsibility to regularly monitor surveillance activity undertaken by the council which falls outside of RIPA. This is in line with guidance from the OSC.

However, it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Councils processes and procedures.

What are the origins of RIPA?

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

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

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

These three points are clarified further in the next paragraphs.

When we talk of interference being "in accordance with the law", this means that any such interference is undertaken in accordance with the mechanism set down by the Regulation of Investigatory Powers Act (RIPA for short) and the Home Office Covert Surveillance Codes of Practice. The Codes of Practice deals with the use of Covert Surveillance and the use of persons such as informants and Undercover Officers who gather information in a covert capacity (**Covert Human Intelligence Source or CHIS** for short – refer to Page 10).

However, a considerable amount of observations are carried out in an overt capacity by Council employees carrying out their normal functions such as parking enforcement, general patrolling etc. These activities are general and routine and do not involve the systematic surveillance of an individual. RIPA is not designed to prevent these activities or regulate them.

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

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

- benefit fraud
- environmental health
- housing
- planning
- criminal investigations by audit such as fraud offences

- envirocrime

RIPA aims to provide a framework to control and supervise covert activities such as surveillance and the use of a CHIS in these criminal investigations. It aims to balance the need to protect the privacy of individuals against the need to protect others by the Council complying with its enforcement functions. There are two separate Codes of Practice, Covert Surveillance and CHIS.

Any covert activity carried out under this legislation must meet the test of necessity and proportionality. These are dealt with on page 22 of this policy.

When Does RIPA Apply and Who Does it Apply to?

RIPA applies to public authorities such as local authorities and permits them to conduct COVERT Surveillance activities and use Covert Human Intelligence Sources (CHIS) such as informants and undercover officers (see pages 10 to 15). However, on 1 November 2012, two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments contained in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of **Directed Surveillance** where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

The crime threshold, as mentioned is only for Directed Surveillance.

Therefore the only lawful reason for Directed surveillance to be authorised is for the **prevention and detection of crime.** As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour unless there are criminal offences involved which attract a maximum custodial sentence of six months.

RIPA and this policy also apply to any contract staff employed by the Council to undertake such activity covered by the codes.

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

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

Private information

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

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

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

If you need to conduct surveillance or use a CHIS as part of investigating a criminal matter which might result in court proceedings or proceedings before some other form of tribunal, you should consider whether private information is likely to be gained as a result of the activities and whether RIPA applies.

WHAT HAPPENS IF RIPA IS IGNORED?

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

The person who was the subject of your surveillance may also complain to the Ombudsman who may order the Council to pay compensation. The activity may also be challenged through the civil courts under the Human Rights Act 2000 for breach of privacy.

There is also a requirement to report errors to the OSC, such as surveillance activity which should have been authorised but which was carried out outside of RIPA. (See section on errors)

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

Surveillance outside of RIPA

Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that a local authority can now only grant an authorisation under RIPA where the local authority is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

There may be a necessity for the Council to undertake surveillance which does not meet the criteria above to use the RIPA legislation such as in cases of serious disciplinary investigations or anti-social behavior.

The Council still must meet its obligations under the Human Rights Act and therefore any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be well documented The Office of Surveillance Commissioners Procedures and Guidance 2011 states that it is prudent to maintain an auditable record of decisions and actions to use covert surveillance without the protection of RIPA and that such activity should be regularly reviewed by the SRO.

The Councils Senior Responsible Officer (SRO) will therefore regularly monitor surveillance outside of RIPA. Before any such surveillance takes place advice must be sought from Legal Services.

As part of the new process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form should be completed and authorised by at least a tier 4 level manager. A copy of the non RIPA surveillance application form can be found on the Intranet or is available from the RIPA Monitoring Officer.

Non RIPA surveillance also includes staff surveillance which falls outside of RIPA. Any surveillance of staff must be formally recorded on the non-RIPA surveillance Application Form and authorised by the Head of Service in consultation with the Head of Internal Audit. A central record of staff surveillance is also maintained by the SRO.

What is Surveillance?

Surveillance:

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

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

Covert Surveillance:

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

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

If activities are open and not hidden from the persons subject to surveillance such as Officers conducting Council business openly, e.g. a market inspector walking through markets, the RIPA framework does not apply because that is "Overt Surveillance". Equally, if you tell the subject that surveillance will be taking place, the surveillance is overt. This would happen, for example, where you warn a noisemaker that noise will be recorded if it continues. RIPA does not regulate Overt Surveillance. Remember it is the Council's responsibilities to ensure that whatever action is taken is compliant with the Human Rights Act and is a necessary and proportionate response to the issue being dealt with.

RIPA regulates two types of Covert Surveillance which are

- **Directed Surveillance**
- **Intrusive Surveillance**

Directed surveillance:

Directed Surveillance is defined in paragraph 2.2. of the Revised Codes of Practice as follows:

Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation);

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

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

Immediate response to events

There may be occasions when officers come across events unfolding which were not pre planned which then requires them to carry out some form of observation. This will not amount to Directed Surveillance. However, it will amount to surveillance outside of RIPA and must still be necessary and proportionate and take account of the intrusion issues. Officers must not abuse the process and be prepared to explain their decisions in court should it be necessary. It is important when conducting surveillance in these circumstances that officers still understand that they have obligations to ensure that their actions are Human Rights Act compliant and are therefore necessary and proportionate and take account of the intrusion issues. Therefore they should document their decisions, what took place, and what evidence or information was obtained.

Recording of telephone conversations

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

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

Intrusive surveillance:

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

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

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

Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on

the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

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

Commercial premises and vehicles

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

The Council has no authority in law to carry out Intrusive Surveillance or activity under the Police Act 1997.

Covert Human Intelligence Source (CHIS)

A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as sources. However, it is possible that members of the public, whom repeatedly supply information to Council staff on either one particular subject or investigation or a number of investigations, may become a CHIS. It is important that Council staff make the necessary enquiries of the person reporting the information to ascertain how the information is being obtained. This will not only assist with evaluating the information but will determine if the person is establishing or maintaining a relationship with a third person to obtain the information, and then provide it to the Council staff. If this is the case, the person is likely to be acting as a CHIS and there is a potential duty of care to the individual which a duly authorised CHIS would take account of. Therefore Council staff should ensure that they are aware of when a person is potentially a CHIS by reading the below sections. If further advice is required contact the RIPA Coordinator/Legal Adviser.

Under section 26(8) of the 2000 Act a person is a source if:

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

b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

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

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

Conduct and Use of a Source

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

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

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

When completing applications for the use of a CHIS you are stating who the CHIS is, what they can do and for which purpose

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

Management of Sources

Within the provisions there has to be;

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare **(Handler)**

(b) at all times there will be another person who will have general oversight of the use made of the source **(Controller)**

(c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

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

- dealing with the source on behalf of the authority concerned;

- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare;

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

Tasking

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

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

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

Management Responsibility

The Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

The Handler of the source will usually be of a rank or position below that of the Authorising Officer.

It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be necessary the CHIS Codes of Practice should be consulted to ensure that the Council can meet its management responsibilities.

Security Welfare and Confidentiality

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

The confidentiality of the CHIS is paramount and consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in court.

CHIS and Test Purchases

Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would **not** normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and directed surveillance. However, both directed surveillance and CHIS application forms will need to be completed and authorisation obtained. The forms should also be cross referenced.

CHIS and ANTI-SOCIAL BEHAVIOUR

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

CHIS and EXCEPTIONS

A source, whether or not wearing or carrying a surveillance device and invited into residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or vehicle which take place in his presence. This also

applies to the recording of telephone conversations other than by interception which takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way.

MAKING USE OF CHIS INTELLIGENCE DATA

Material obtained from a source may be used as evidence in criminal proceedings. Furthermore, the product obtained by a source described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996. There are also well-established legal procedures that will protect the identity of a source from disclosure in such circumstances. Information obtained from a CHIS must be processed in the same way the product of a Directed Surveillance operation is handled and stored. Access to the information must be restricted and the confidentiality of the CHIS maintained.

Record Management for CHIS

Proper records must be kept of the authorisation and use of a source. The particulars to be contained within the records are;

a. the identity of the source;

b. the identity, where known, used by the source;

c. any relevant investigating authority other than the authority maintaining the records;

d. the means by which the source is referred to within each relevant investigating authority;

e. any other significant information connected with the security and welfare of the source;

f. any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

g. the date when, and the circumstances in which, the source was recruited;

h. the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

i. the periods during which those persons have discharged those responsibilities;

j. the tasks given to the source and the demands made of him in relation to his activities as a source;

k. all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

l. the information obtained by each relevant investigating authority by the conduct or use of the source;

m. any dissemination by that authority of information obtained in that way; and

n. in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

All original surveillance authorisation (whether authorised or refused), Review, Renewal and Cancellation documents will be forwarded to the RIPA Legal Advisor. The RIPA Legal Advisor will be responsible for maintaining the Central Record of Authorisations (see Documentation and Central Record page 26) and will ensure that all records are held securely with no unauthorised access. The only persons who will have access to these documents will be the RIPA Coordinator/Legal Advisor and the Director of Legal and Democratic Services Section.

Contact details for RIPA Legal Advisor

Name	Job Title	Extension number
Mike Richardson	Lawyer	9409

RIPA Application and Authorisation Process

As mentioned earlier on 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (“the 2010 Order”) mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco

under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

This crime threshold, as mentioned, is only for Directed Surveillance.

Application, Review, Renewal and Cancellation Forms

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP's approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows;

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP's approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete the required section of the aoolication for judicial approval form. Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

It will then be necessary for the applicant to contact Her Majesty's Courts & Tribunals Service (HMCTS) (within Office hours) to arrange a hearing at the Magistrates' Court, to apply to a JP to grant an order approving the authorisation. The hearing will be in private and heard by a single JP.

Officers who may present the authorisations will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the RIPA Coordinator/Legal advisor

Upon attending the hearing, the officer must present to the JP the partially completed application for judicial approval form, a copy of the RIPA authorisation form, together with any supporting documents setting out the case, and in the case of a renewal the original authorisation form.

The original RIPA authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' Officers and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA authorisation and the application for judicial approval form. They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the authorisation form**. However, the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided**.

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to:

Approve the Grant or renewal of an authorisation
The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case.

Refuse to approve the grant or renewal of an authorisation
The RIPA authorisation will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation or notice

This applies where the JP refuses to approve the authorisation or renew the authorisation and decides to quash the original authorisation or notice. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case the officer will inform Legal Services who will consider whether to make any representations.

Whatever the decision, the JP will record their decision on the order section of the judicial approval form. The court administration will retain a copy of the local authority RIPA authorisation form and the judicial approval form. The officer will retain the original authorisation and a copy of the judicial approval form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date. The officers are now allowed to undertake the authorised activity.

The original application and the copy of the judicial approval form should be forwarded to the the Central Register and a copy retained by the applicant and by the AO. This will enable the AO to check what was authorized and monitor any reviews and cancellation to determine if any errors occurred and if the objectives were met.

There is no complaint route for a judicial decision unless it was made in bad faith. If the applicant has any issues they must contact Legal Services for advice. A local authority may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal team will decide what action if any should be taken.

All the relevant forms for authorisation through to cancellation must be in writing using the standard forms which are available from the Intranet site and from the RIPA Coordinator/ Legal Adviser, but officers must ensure that the circumstances of each case are accurately recorded on the application form (see Application Process).

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

An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference (see collateral intrusion on page 23). The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

Applications

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

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. Where appropriate, the Line Manager will perform an initial quality check of the application and/or legal advice sought. Completed application forms are to be initialed by Line Managers to show that the quality check has been completed.

Applications whether authorised or refused by the Authorising Officer will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations.

If authorised the applicant will then complete the relevant section of the application for judicial approval form and follow the procedure above by arranging and attending the Magistrates Court to seek a JP's approval. (see procedure above RIPA application and authorisation process)

Duration of Applications

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

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire. (See cancellations page 20)

Reviews

The reviews are dealt with internally by submitting the review form to the Authorising Officer. There is no requirement for a review form to be submitted to a JP.

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

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

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. If the circumstances or the objectives have changed considerably, or the techniques to be used are now different a new application form should be submitted and will be required to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

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

Renewal

Should it be necessary to renew a Directed Surveillance or CHIS authorisation this must be approved by a JP.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors, which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the Authorising Officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

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

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraph 5.18 in the Codes of Practice). It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by the RIPA Legal Advisor.

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

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

Who Can Grant a RIPA Authorisation?

Officers who are designated "Authorising Officers" may authorise the use of directed surveillance or the use of a CHIS whether on a written application or under the urgency oral procedures.

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

The Chief Executive Officer or in his absence the Executive Director of Children and Adults Services will authorise cases where confidential information is likely to be gathered or in the case of a juvenile or vulnerable CHIS.

The Director of Legal and Democratic Services will inform the RIPA Legal Advisor of any changes to the list of Authorising Officers and will amend the policy accordingly. The intranet will also be updated appropriately.

Urgent Oral Authorisations

As from 1 November 2012 there is now no provision under RIPA for urgent oral authorisations.

Local Sensitivities

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

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

Authorising Officers Responsibility

Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable such as where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation the Central Record of authorisations (see page 26) should highlight this and it should be brought to the attention of a Commissioner or Inspector during their next inspection.

Authorising Officers must treat each case individually on its merits and satisfy themselves that the authorisation is in accordance with the law, **necessary** for the prevention and detection of crime, that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

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

Authorising Officers are responsible for determining when reviews of the activity are to take place. (See Reviews on page 19).

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

Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should the Authorised Officer approve any RIPA form unless, and until they are satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed.

Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the latest Procedures and Guidance from the Office of Surveillance Commissioner (OSC). This latter document details their latest guidance to be followed and Authorising Officers are required to hold their own copy.

Before authorising surveillance/use of CHIS, Authorising Officers must be mindful of this policy, training provided by the council and any other guidance issued from time to time.

When authorising the conduct or use of a CHIS, Authorising Officers must also be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved; be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment and consider any adverse impact on community confidence that may result from the use or conduct or the information obtained.

In the absence of the Director of Legal and Democratic Services the Application should be submitted to another Authorising Officer for authorisation. (See list of Authorising Officers - Appendix 1)

Necessity and Proportionality

Obtaining a RIPA authorisation will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. It must be necessary for the **prevention and detection of crime and that** the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. It must also be shown the reasons why the requested activity is necessary in the circumstances of that particular case. Can you achieve the same end result without the surveillance?

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

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

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

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

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

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

Collateral Intrusion

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

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

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

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

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

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

The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but you should weigh up the importance of the activity to be carried out in operational terms on the one hand and the risk of collateral intrusion on the other hand.

Unexpected Interference with Third Parties

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

Confidential Information

Confidential information consists of matters subject to Legal Privilege, confidential personal information or confidential journalistic material and applications where there is a likelihood of acquiring such information can only be authorised by the Chief Executive
No authorisation should be authorised if there is any likelihood of obtaining legally privileged material without consulting the Legal Services.

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

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

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

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

- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Director of Legal and Democratic Services) 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.

Use of CCTV

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

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

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

Internet Investigations

The use of the internet as an investigative method is now becoming routine. However, just because the information being obtained is from the internet staff must still consider all the normal rules and guidance applicable to any type of enquiry conducted within a criminal investigation, such as, the Data Protection Act (DPA), Criminal Procedures Investigations Act (CPIA) and RIPA. In the Surveillance Codes of Practice issued December 2014 there is now a section dealing with these types of enquiries. Therefore the paragraph titled Online Covert Activity at section 2.29 has been replicated and should be taken into consideration should staff wish to carry out internet open source enquiries, particularly where Social Networking Sites are involved.

2.29 The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought as set out elsewhere in this code. Where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

If staff wish to conduct internet enquiries, particularly Social Networking Sites they must consider the intrusion issues on the subject of the enquiries and other innocent people (collateral intrusion) and when obtaining the evidence this must be stored in line with the Data Protection Act. They must also consider whether they are monitoring in line with the surveillance definition. If so, and they are likely to obtain private information they are likely to require authorisation under the RIPA legislation. These activities are forming part of the RIPA inspections and will also be audited internally.

Urgent Authorisations

As from 1 November 2012 there is no provision under RIPA for urgent oral authorisations.

Joint Agency Surveillance

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

Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application to carry out the activity. When staff are operating on another organisations authorisation they should obtain either a copy of the application form (redacted if necessary) or a copy of the authorisation, containing the unique number. This will ensure they see what activity they are authorised to carry out. Their line manager should be made aware of the joint surveillance and a copy of the authorisation forwarded to the central register in order that a record can be retained. This will assist with oversight of the covert activities undertaken by Council staff.

Provisions should also be made regarding any disclosure implications under the Criminal Procedures Act (CPIA) and the management, storage and dissemination of any product obtained.

Documentation and Central Record

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

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

- If refused, that the application was not authorised and a brief explanation of the reason why. The refused application should be retained as part of the Central Record of Authorisation.
- if granted, the type of authorisation and the date the authorisation was given and approved by the JP;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- frequency and the result of each review of the authorisation;

- if the authorisation is renewed, when it was renewed, the name and rank/grade of the authorising officer; and the date approved by the JP.
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorisation was cancelled.
- Up until the 1st November 2012 authorisations by an Authorising Officer in urgent cases where they are directly involved in the investigation or operation (see Authorising Officer Responsibility page 21.) If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.
- the date and time when any instruction was given by the Authorising Officer.

As well as the Central Record the RIPA Legal Advisor will also retain:

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

For CHIS applications the Codes state;

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

- the original authorisation form together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- the original renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;

- the reasons for cancelling an authorisation.

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

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

Annual Report to Office of Surveillance Commissioners

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

Storage and Retention of Material

All material obtained and associated with an application will be subject of the provisions of the Criminal Procedures Investigations Act 1996 (CPIA), Codes of Practice which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances. It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of the Data Protection Act

All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained together with relevant associated paperwork should be held securely and ensure any dissemination of the product takes account of the DPA and is only disclosed to those that can lawfully receive it. The material may only be retained for as long as is necessary, therefor material which will be retained outside of the CPIA provisions (see below) must have some justification to meet the DPA requirements. If in doubt advice should be sought from the Data Information Governance Manager

Extra care needs to be taken if the application and material relates to a CHIS (see page 10 to 15)

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

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

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

Departments making use of Directed Surveillance operations must ensure procedures are in place for the secure handling, storage and subsequent destruction of the product of the surveillance. Whilst each department will have its own internal procedure for the handling of evidence, below is a non-exhaustive list of factors which should be considered.

- Details of the product of surveillance must be recorded including the date, time and place the product was obtained and the operation to which it relates.
- The product must be kept in secure storage with access to the product restricted.
- The movements of the product must be recorded. If the product is removed from storage, the time, date and reasons for the movement of the product must be recorded; so too the details of the recipient of the product and the person authorising its removal from storage. Similarly, records must be updated when the product is returned to storage and when the product is destroyed.
- Any product that is deemed to be of no use in proceedings must be destroyed immediately. If the product is used as evidence in proceedings, it must be securely stored and destroyed with the additional evidence in accordance with the department's internal procedures.

Training

There will be an ongoing training programme for Council Officers who will need to be aware of the impact and operating procedures with regards to this legislation. The training officer will be required to retain a list of all those officers who have received training and when the training was delivered.

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

Errors

There is now a requirement as set out in the OSC procedures and Guidance to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't.

This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. (See oversight section below)

Oversight

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

Reporting to Members

Quarterly returns of all surveillance activity undertaken by Council staff including joint surveillance and Directed Surveillance using the CCTV system will be compiled by the RIPA Legal Advisor and reported to the Portfolio Holder for Finance and Performance in line with the current advice in the Codes of Practice. Members will review on a yearly basis the policy to assess whether the activity undertaken is in line with this policy.

Scrutiny and Tribunal

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

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

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

Complaints can be addressed to the following address

Investigatory Powers Tribunal
PO Box 33220
London
SW1H9ZQ

Appendix 1

APPROVED LIST OF AUTHORISED OFFICERS FOR DIRECTED SURVEILLANCE AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

- **Head of Regulatory services**

  Mark Wiltshire

- **Head of Audit and Investigations**

  Steven Tinkler

- **Head of Legal Property and Regulatory**

  Jackie Adams

IMPORTANT NOTES

1. Only the Chief Executive or in his absence Executive Director of Children and Adults Services are authorised to sign Forms relating to Juvenile Sources and Vulnerable Adults.