Appendix 1

PROCEDURAL NOTE INDEX

PROCEDURAL NOTE & AUTHORISATION FRAMEWORK FOR RIPA 2000 – SURVEILLANCE ACTIVITIES

1. INTRODUCTION

The *Regulation of Investigatory Powers Act 2000 ("RIPA")* came into force in England on 25 September 2000. It pre dated the introduction of the *Human Rights Act 2000 ("HRA")* by a week.

The main purpose of RIPA was to ensure that the relevant investigatory powers are used and exercised in accordance with the HRA and the European Charter on Human Rights ("ECHR") in an attempt to stem a possible raft of appeals to Europe over improper use of investigative powers. RIPA was enacted to comply, in particular, with the right to private life (Article 8) and the right to a fair trial (Article 6) of the ECHR.

RIPA is not comprehensive, for example surveillance by private organisations or individuals and general CCTV is not covered by the Act.

If surveillance undertaken by the Council is not properly authorised, it may be subject to legal challenge.

The authorisation procedure outlined in this note does not preclude a challenge to the legality of the surveillance. For example, the fact that the officer who authorised surveillance believed that the action authorised was proportionate to what is sought to be achieved does not mean that a Court would take the same view.

However, it is thought that activities that interfere with private life and which are carried out in accordance with the authorisation procedures in RIPA are likely to be HRA compliant and able to withstand legal challenge. Breach of the RIPA authorisation procedures may give rise to exclusion of the evidence gathered due to a lack of authorisation or improperly authorised surveillance.

The relevant Investigatory powers under RIPA are:-

- Directed surveillance in the course of specific operations
- The use of covert human intelligence sources (agents, informants, undercover officers)

1.1 Why might the Council want to undertake covert surveillance?

- To establish facts relevant to the business of Council
- To ascertain employees compliance with the law and self regulatory polices or procedures
- To prevent or detect crime

- To ascertain whether employees are meeting the organisations standards
- To monitor only, whether or not communications are business related
- To detect harassment or other inappropriate behaviour by employees
- Monitor employee performance (for example, if they are spending too much time on the internet or sending private emails)
- Monitor and detect the outward transmission of trade secrets and confidential information
- Detect signs of a stress related problem in an employee
- Employee malingering – e.g. keyboard monitoring
- To protect public health
- In the interests of public safety
- For the purposes of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department

1.2 Who will the authorised officers be?

The authorising officers specified in the Act for Local Authorities are Assistant Chief Officer or Senior Officer of Investigating section depending on the level of authorisation required.. The following members of staff within each area of Council have been appointed as authorising officers:

Chief Internal Auditor – Finance Department.

Benefit Investigation Manager – Housing Benefits Investigations

Director of Childrens Services

Director of Adult Social Services

Director of Environment & Conservation

Assistant Director (Public Protection) – Public Protection.

Assistant Director (Housing Needs) – Housing Needs.

However, if the investigation or operation involves confidential information, the authorisation should be given by the Head of Paid Service or in her absence a Chief Officer. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

2. DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

This is the section of RIPA which is probably of most immediate impact upon the Council and it's activities.

Two types of activity are relevant:-

1. Directed Surveillance
2. Covert human intelligence sources

The definitions of Surveillance – for Council's purposes.

2.1 Directed Surveillance

This is defined to be:-

Directed surveillance is defined in section 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and undertaken:

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

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

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

The Code of Practice published on Covert Surveillance (a copy of which is attached and should be read and referred to by all Officers concerned) gives guidance on what might amount to directed surveillance:-

'General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime "hot spot" in order to identify and arrest offenders committing crime at that location. Trading standards of HM Customs & Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday

functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act. Neither do the provisions

of the 2000 Act or of this Code of Practice cover the use of covert CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime.'

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

'Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. Such activity is defined as "intrusive surveillance" in RIPA. However, where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle (a tracking device), the activity is classed as directed surveillance and should be authorised accordingly. Directed surveillance does not include entry on or interference with property or wireless telegraphy.'

2.1.1 Authorisation of directed surveillance

Authorisation will provide lawful authority for a public authority to carry out directed surveillance.

Authorisation for directed surveillance may be granted by people holding the rank etc of *'Assistant Chief Officer'* or *'Officer responsible for the management of an operation'* within the London Borough of Islington. Application form(s) for the granting of authorisation are attached to this note.

Section 28 of RIPA provides that an authorisation cannot be granted unless specific criteria are satisfied, namely, that the person granting the authorisation believes that:-

a. The authorisation is necessary on a *specific ground;*

The *specific grounds* which may make an authorisation necessary is:-

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

AND

b. The authorised activity is proportionate to what is sought to be achieved by it.

There is no specific guidance on what exactly is meant by this requirement. However, it is likely that a Court would look, in reviewing a decision of an authorising officer, at whether the proposed method of surveillance does not constitute 'overkill' e.g. a large surveillance operation involving six officers for two months investigating housing benefit fraud worth £100.00.

The Code of Practice should be consulted by the authorising officer and the investigating officer both when completing the application form and when deciding whether to authorise such surveillance.

It is important to note that the conduct and activities that are authorised by an authorisation for the carrying out of directed surveillance is any conduct that is described and carried out for the purposes of the investigation or operation specified and described in the authorisation.

2.1.2 Use of Private of Investigators

The Authority on occasions instructs Private Investigators to undertake directed surveillance. The officer in the case wishing to instruct a Private Investigator should follow the procedure set out below:-

(i) The officer should mention the use of the PI in the application for authorisation.

(ii) The PI in the letter of instruction should be made aware of the parameters of the surveillance activity.

(iii) The PI should be instructed to handover all surveillance material obtained.

(iv) The officer in the case should check with the PI at the conclusion of the surveillance that all surveillance material has been handed over to the Authority.

2.2 Covert Human Intelligence Source

Some key definitions are:-

Covert surveillance is covert if it is carried cut in a manner that is calculated to ensure that people who are subject to the surveillance are unaware that it is or may be taking place.

Covert purpose, in relation to the establishment or maintenance of a personal or other relationship, if the relationship is conducted in a manner that is calculate to ensure that one of the parties to the relationship is unaware of the purpose.

Covert relationship is one in which the information obtained is disclosed covertly 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.

A covert human intelligence source is effectively an inside informant or undercover officer, i.e. someone who develops or maintains their relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator.

The definition in RIPA is as follows:-

A person is a **covert human intelligence source** if:-

(a) s/he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything below:-

- s/he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

- s/he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship

The 'use' of covert human intelligence source is a reference to inducing, asking or assisting a person to engage in the conduct of such a source, or to obtain information by means of the conduct of such a source.

The material obtained from the use or conduct of a source can be adduced as evidence in Court proceedings. There are well established legal procedures which, at the Court's discretion, will protect the identity of the source in such circumstances.

2.2.1 Authorisation of Covert Human Intelligence Sources

Authorisation for CHIS may be granted by people holding the rank etc of *'Assistant Chief Officer'* or *'Officer responsible for the management of an operation'* within the London Borough of Islington. Application forms for the granting of authorisation are attached to this form.

Section 29 of the RIPA provides that an authorisation can not be granted unless specific criteria are satisfied, namely, that the person granting the authorisation believes that:-

a. The authorisation is necessary on a *specific ground*;

The *specific ground* which may make an authorisation necessary is:-

- For the purposes of preventing or detecting crime or preventing disorder

AND

b. **The authorised activity is proportionate to what is sought to be achieved by it**

There is no specific guidance on what exactly is meant by this requirement. However, it is likely that a Court would look, in reviewing a decision of any authorising officer, at whether the proposed method of surveillance does not constitute 'overkill' e.g. a large surveillance operation involving six officers for two months investigating housing benefit fraud worth £100.00.

And that there is in place a system ensuring:

That there is a separation of roles between the authorising officer, investigating officer and record keeper, they cannot all be the one person. Specifically, the authorising officer must ensure that there is.

c. Day to day supervision of the source

That there will be at all times a person holding an office, rank or position within the Council who will have day-to-day responsibility for dealing with the source on behalf of the Council, and for the sources security and welfare

d. General oversight of the Source

That there will be at all times another person holding an office, rank or position within the Council who will have general oversight of the use made of the source

e. Records relating to the Source

That there will be at all times a person holding office, rank or position with the Council who will have responsibility for maintaining a record of the use made of the source.

f. Release and access of those records

That records maintained by the Council that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to such persons.

It is imperative that the authorising officer is satisfied in granting the authorisation that there are at least two but preferably three people who are aware of and understand their role in relation to the source. The one person ('the controller') who is dealing day to day with the source cannot be both the record keeper and the general overseer. The controller can be the record keeper but cannot, be the authorising officer and/or the person charged with overseeing the whole operation.

The detail of what must be stored within the records kept is outlined in the *Code of Practice on the Use of Covert Human Intelligence Sources* which is attached.

Special attention must be paid to the *Code of Practice on the Use of Covert Intelligence Sources* when 'cultivating' a source and using juvenile sources etc.

The conduct and activities that are authorised by an authorisation for the carrying out of covert surveillance is any conduct that is described and carried out for the purposes of the investigation or operation specified and described in the operation.

2.3 Grant, renewal, cancellation and duration of authorisations

2.3.1 Grant and duration

In urgent cases an authorising officer may give an oral authorisation. The duration of such an authorisation is 72 hours, at which time there must be an application on the appropriate attached form for renewal. In such cases, the relevant Code suggests that a statement that the authorising officer has expressly authorised the action should be recorded in writing and dated as soon as is reasonably practicable. This should be done by the person to whom the authorising officer spoke but should later be endorsed by the authorising officer.

All other authorisations must be in writing on the appropriate application forms. All sections of the application form must be completed and should there be any queries with how to fill out the forms, this procedural note and the attached *codes of Practice* should be consulted for guidance.

An authorisation for directed surveillance, made in writing is valid for three months.

An authorisation for the conduct or the use of a covert human intelligence source, made in writing, is valid for 12 months from the date of grant. Should the surveillance be continuing beyond this time, a renewal on the appropriate form must be applied for prior to the expiry of the authorised term.

2.3.2 Renewal

A renewal of any authorisation may be made at any time before the time at which it ceases to have effect, by any person who would be entitled to grant the authorisation in the same terms.

An authorising officer cannot renew an authorisation for the conduct and use of a covert intelligence source unless he/she is satisfied that a review has been carried out of:
(a) the use of the source in the period since the grant or latest renewal

(b) the tasks given to the source during that period and the information obtained from the conduct or the use of the source

and upon receipt of this information has considered the results of the review for the purpose of deciding upon the renewal.

2.3.3 Cancellation

The authorising officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that he reasons given for the granting of the authorisation no longer apply. (See attached cancellation forms)

A checklist for completing the required authorisation documents is attached at **Annex 1**.

2.3.4 Records

Central Record of RIPA Authorisation and other records to be maintained by the Authority

The Covert Human Intelligence Sources Code of Practice and the Covert Surveillance Code of Practice (both of which came into force on August 2002) recommend that a centrally retrievable records of all authorisations should be held by each public authority.

The Inspector from the Office of Surveillance Commissioners recommended to the Authority in August 2002 that a central record of authorisations should be created under the supervision of a Senior Officer.

The authority has decided that the central record of authorisations will be maintained by internal audit and the Chief Internal Auditor will be the Senior Officer with supervisory responsibility.

The Central Record

A centrally retrievable record of all authorisation should be held by the authority and regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant commissioner or an inspector from the Office of Surveillance Commissioners, upon request. These records be retained for a period of at least three years from the ending of the authorisation and should contain the following information:

- the type of authorisation
- the date the authorisation was given;
- 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;
- 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.

Forwarding information to Internal Audit

The officer in the case should complete the central record authorisation proforma and send it to internal audit. The auditor will enter the information on the central record. An example of the proforma is attached at **Annex 2**.

Other records to be maintained by the Authority

In all cases, the authority should maintain the following documentation which need not form part of the centrally retrievable record:

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

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

- the frequency of reviews prescribed by the authorisation officer;

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

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

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

Covert Human Intelligence Sources

The code of practice states, as for covert surveillance, that a centrally retrievable record of all authorisation should be held by the authority and regularly updated whenever authorisation is granted, renewed or cancelled. The record should also be made available to the relevant commissioner or an inspector from the office of Surveillance Commissioners and the record should be retained for a period of at least three years from the ending of the authorisation. It will be appropriate for the central record to contain the same information as required for covert surveillance (as listed above).

Proper records must be kept of the authorisation and use of a source. An authorising officer must not grant an authorisation for the use or conduct of the source unless he

believes that there are arrangements in place for insuring that there is at all times a person with the responsibility for maintaining a record of the use made at the source.

In addition the authority should maintain records or copies of the following as appropriate, which need not form part of the centrally retrievable record:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of authorisation, together with the supporting documentation submitted wen 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 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 authorised officer to cease using the source.

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

All records should be retained for a minimum of three years to ensure that they are available for inspection by a Commissioner or an Inspector from the Office of Surveillance Commissioners upon request. Thereafter, material must not be destroyed except with the authority of the authorising officer. The authorising officer is held accountable for the storage, maintenance and destruction of the records and authorisations.

Should there be a reasonable belief that material relating to any activity by a source could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with existing disclosure requirements deriving from the *Police and Criminal Evidence Act 1992*.

2.3.5. Monitoring and Quality Control

The Chief Executive has overall responsibility for monitoring the Authority's use of the Legislation. The Chief Internal Auditor is to report to her on a quarterly basis the number of authorisations granted, renewed and cancelled and the quality of the authorisations.

The Chief Internal Auditor has responsibility for the maintenance of the Central Record of Authorisations. This record will provide information for the quarterly monitoring report.

The Chief Internal Auditor will arrange audits of Council Departments surveillance records to assess the quality of authorisation.

3. Accessing Communications Data

3.1 What is communications data ?

Communications data is information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself, contents of e-mails or interactions with website.

Communications Data is defined in Section 21(4) RIPA 2000 as follows:

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it has been or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)and is about the use made by any person -

(i) of any postal service or telecommunication service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of the telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing the postal service or telecommunications service.

A Local Authority can only access communications data falling within sections 21(4)(b) and (c).

3.2 Applications to obtain communications data

An application to obtain communications data must be authorised by a senior member of staff within the Local Authority. The authorising officer (designated

person) should be an Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent.

3.2.1 Authorisations and Notices

The Act provides two different ways of authorising access to communications data; by an authorisation under Section 22 (3) and by a notice under Section 22 (4) RIPA 2000. An authorisation would allow the Local Authority to collect or retrieve the data itself. A notice is given to a postal telecommunications operator and requires that operator to collect or retrieve the date and provide it to the Local Authority which serves the Notice. A designated person decides whether or not an authorisation should be granted or a notice given.

A Section 22(3) authorisation may be appropriate where:-

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- There is a prior agreement in place between the relevant Local Authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

Applications to obtain communications data should be made on the standard directed surveillance authorisation form which must be retained by the Local Authority until it has been audited by the Commissioner.

The Application Form should subsequently record whether access to communications data was approved or denied, by whom and the date.

<u>Considerations for Designated Person</u>

Access to communications data can only be authorised by a Local Authority for the purpose of preventing or detecting crime or preventing disorder.

The designated person will need to be satisfied that obtaining the telecommunications data is necessary for the purpose as set out above.

The designated person will need to consider whether obtaining access to the data is proportionate to what is sought to be achieved.

The designated person must take into account where appropriate, when accessing the communications data is likely to result in collateral intrusion, whether the circumstances of the case still justify that access and whether any urgent time scale is justified.

A designated person will make a decision whether to issue a notice or an authorisation based upon the application which is made. If a notice is issued

this is served on the holder of the communications data and should be in the standard format.

3.3 Validity of Authorisations and Notices.

Authorisations and notices will only be valid for one month. The designated person should specify a shorter period if that is justified by the request, since this may go to the proportionality requirements. For "future" communications data disclosure may only be required of data obtained by the postal or telecommunications operator within this period i.e. upto one month. For "historical" communications data disclosure may only be required of data in the possession of the postal or telecommunications operator. The postal or telecommunications operator should comply with the notice as soon as it is reasonable practicable. They will not be required to supply data unless it is reasonably practicable to do so.

An authorisation or notice may be renewed at any time during the month it is valid, by following the same procedure as in obtaining a fresh authorisation or notice. A renewed authorisation or notice takes effect at the point which the authorisation or notice it is renewing expires.

A designated person should cancel a notice as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. In the case of a notice, the relevant postal or telecommunications operator will be informed of the cancellation.

3.4 Single Point of Contact

Notices and were appropriate authorisations for communications data should be channelled through Single Points of Contact within the Local Authority. The Single Points of Contact will deal with the postal or telecommunications operator on a regular basis. The Authority will be able to have Single Points of Contact in each service area. Officers acting as the Single Point of Contact (SPOC) will need to be trained on a course recognise by the Home Office. After 6th June 2004 the telecommunication companies will only liaise with trained authorised SPOC.

3.5 Retention of Records.

Applications, authorisations and notices for communications data must be retained by the Local Authority until it has been audited by the Commissioner. The Local Authority should keep a record, of the dates on which the authorisation or notice is started and cancelled.

The Officer in the case should complete the central record authorisation pro forma and send it to internal audit. The auditor will enter the information on the central record, an example of the pro forma is attached at annex 3.

Where any errors have occurred in the granting of authorisations or the giving of notices, a record should be kept and a report and explanation sent to the Commissioner as soon as it is practical.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely.

4. CONCLUSION

Should the guidelines and framework outlined in this note be adhered to by Council, it is likely to mean that any evidence gathered by such surveillance will be admissible in any Court or Tribunal and that the Council will not be liable either under criminal or civil law for acts done in the course of authorised surveillance.

A summary document has been prepared and attached. The contents of this note and the Codes of Practice should be read and discussed by all investigators, authorising officers and records officers so that the contents and procedures are fully understood. Some thought should be given for an appropriate 'back up' or 'reserve' system should the nominated authorising officer not be available. The 'back up' authorising officer should be of appropriate rank or position as specified under RIPA and be conversant with the duties and responsibilities.

Should there be any issues in the implementation of these RIPA procedures, please do not hesitate to contact Legal Services.

5. SOURCE LEGISLATION

5.1 Legislation

Regulation of Investigatory Powers Act 2000 (RIPA 2000)
Human Rights Act 1998
Data Protection Act 1998 – Use of surveillance data

5.2 Statutory Instruments and Codes

The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000 SI 2000 No. 2417
The Regulation of Investigatory Powers Act 2000 (Commencement No. 1 and Transitional Provisions) Order 2000 SI 2000 No. 2665
The Regulation of Investigatory Powers (Notification of Authorisations etc) Order 2000 SI 2000 No 2563
The Investigatory Powers Tribunal Rules 2000 SI 2000 No 2665
The Regulation of Investigatory Powers (Source Records) Regulations 2000 SI 2000 No. 2725

The Regulation of Investigatory Powers (Juveniles) Order 2000 SI 2000 No. 2793
The Regulation of Investigatory Powers (Cancellation of Authorisations) Regulations 2000 SI 2000 No. 2794
Code of Practice, the use of covert intelligence sources
Code of Practice, Covert Surveillance
Voluntary Code of Practice for users of CCTV and similar surveillance equipment – issued under provisions of the DPA 1998
Accessing Communications Data Draft Code of Practice 2004.
Regulation of Investigatory Powers (Communications Data) Order 2003
Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003.

6. SUMMARY CHECKLIST

1. If an investigator identifies the need for directed surveillance or covert human intelligence source.

2. He/she must contact the relevant authorising officer for his/her department.

3. The investigator should complete the relevant authorisation form fully.

4. The authorising officer should satisfy him/herself that the proposed surveillance satisfies the criteria within the Procedure Note and relevant Codes of Practice.

5. In the case of covert human intelligence source, the authorising officer must in addition to the other criteria satisfy him/herself that there is:

(a) A person who will have day to day responsibility for dealing with the source;
(b) A person (who can be the authorising officer) who will have the general oversight of the use made of the source.

6. In all cases, the authorising officer, should also be satisfied that there is a person responsible for maintaining and collecting all records to do with the surveillance and authorisation. The authorising officer shall ensure that the officer in the case sends required information regarding the authorisation to Internal Audit to be recorded on the Central Record.

7. The authorising officer(s) will be held accountable for the storage, maintenance and destruction of the records and authorisations.

8. Upon authorisation, the investigating officer is entitled to do the activities for the purposes outlined in the authorisation form for the duration of authorisation.

Annex 1

CHECKLIST FOR COMPLETING AUTHORISATIONS FOR DIRECTED SURVEILLANCE OR COVERT HUMAN INTELLIGENCE SOURCE.

a. Use correct ground(s) for the application
b. Enter sufficient detail of the investigation or operation.
c. Enter sufficient detail regarding the activity proposed.
d. Address the issue of proportionality.
e. Address issue of collateral intrusion and avoid 'rubber stamp' comment.
f. Ensure application signed by the applicant.
g. Authorising Officer should set out clear details of what they are authorising.
h. Authorising Officer should avoid 'rubber stamp' comments.
i. Authorising Officer should record time of when the authorisation was signed.
j. Cancellations should be completed properly.
k. Ensure review documents are used properly (officers should not use Renewal of Authorisation documents).

Authorisations should be for 3 months periods. It is possible to state that the authorisation should be reviewed at shorter intervals. If on review, the authorising officer is satisfied that there is no necessity for the authorisation, it should be cancelled.

Annex 2

REQUEST FOR RIPA SURVEILLANCE AUTHORISATION
TO BE RECORDED ON CENTRAL RECORD

1. Type of Authorisation

Directed surveillance	☐
Intrusive surveillance	☐
Covert Human Intelligence Source	☐
Combined authorisation	☐

2. Date authorisation was given: ……

3. Name and post of the authorising officer:
   Name: ……
   Post: ……

4. URN reference number of investigation or operation: ……

5. Title of the investigation or operation (please include a brief description of the investigation or operation and the names of the subjects of the surveillance [if known])
   ……
   ……

   ……..

Were the urgency provisions used to grant the authorisation?
Yes ☐ No ☐

6. Was the authorisation renewed?
   Yes ☐ No ☐

   If the authorisation was renewed, please give the name and post of the authorising officer.

   Name: ……
   Post ……

7. Is the investigation or operation likely to result in obtaining confidential information?
   Yes ☐ No ☐

8. Date authorisation cancelled: ……

Name of Referring Officer: ……
Position: ……
Service Area: ……
Tel extn: …… Date: ……

Annex 3

REQUEST FOR RIPA SURVEILLANCE ACCESSING COMMUNICATIONS DATA TO BE RECORDED ON CENTRAL RECORD

1. Access to communications data authorised by

   Notice under S22(4) ☐
   Authorisation under S22(3) ☐

2. Start date of authorisation or notice: ……

3. Name and post of the authorising officer:
   Name: ……
   Post: ……

4. URN reference number of investigation or operation: ……

5. Title of the investigation or operation (please include a brief description of the investigation or operation and the names of the subjects of the surveillance [if known])
   ……
   ……

   ……

6. Was the authorisation or notice renewed?
   Yes ☐ No ☐

   If the authorisation was renewed, please give the name and post of the authorising officer.

   Name: ……
   Post ……
   Yes ☐ No ☐

7. Date authorisation or notice cancelled: ……

Name of Referring Officer: ……

Position: ……

Service Area: ……

Tel extn: …… Date: ……