

Amended April 2010,
January 2011, December 2011 and January 2012
(Incorporating Revisions from OSC Procedures and Guidance September 2010)
Amended in December 2011 to incorporate recommendations of the OSC
Amended in January 2012 to incorporate recommendations from Office of Surveillance
Commissioners Inspection Report dated 3 November 2011.

STRATFORD-ON-AVON DISTRICT COUNCIL

CORPORATE POLICY & PROCEDURES DOCUMENT

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

(RIPA)

CONTENTS PAGE

	Page No
A <u>Introduction and Key Messages</u>	3
B <u>Council Policy Statement</u>	4
C <u>Authorising Officer Responsibilities</u>	4
D <u>General Information on RIPA</u>	5
E <u>What RIPA Does and Does Not Do</u>	6
F <u>Types of Surveillance</u>	7
G <u>Conduct and Use of a Covert Human Intelligence Source (CHIS)</u>	10
H <u>Authorisation Procedures</u>	12
I <u>Working with / Through Other Agencies</u>	15
J <u>Record Management</u>	16
K <u>Role of the Monitoring Officer</u>	16
L <u>Concluding Remarks of the Monitoring Officer</u> ..	17

[Appendix 1 - List of Authorising Officer Posts](#)

[Appendix 2 – RIPA Flow Chart](#)

[Appendix 3 – RIPA A Forms : Directed Surveillance](#)

[Appendix 4 – RIPA B Forms : Covert Human Intelligence Source \(CHIS\)](#)

NB:

The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application, this Corporate Policy & Procedures Document refers to 'Authorising Officers'. Furthermore, such Officers can only act under RIPA if they have been duly certified by the Council's Monitoring Officer. For the avoidance of doubt, therefore, all references to duly certified Authorising Officers refer to 'Designated Officers' under RIPA.

Acknowledgement: Birmingham City Council for its work in developing this document.

A. Introduction and Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA') and Home Office's Code of Practices on Covert Surveillance and Covert Human Intelligence Sources (covert surveillance would be used only rarely and in exceptional circumstances).
2. The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this Document should contact, at the earliest possible opportunity, the Monitoring Officer, for advice and assistance. Appropriate training and development will be organised and training given by the Monitoring Officer to relevant Authorising Officers and other senior managers.
3. The Monitoring Officer will maintain and check the Central Record/Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorising Officer, however, to ensure the Monitoring Officer receives the original of the relevant forms within 3 days of authorisation, review, renewal, cancellation or rejection.
4. RIPA and this Document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This Document will, therefore, be kept under 6-monthly review by the Monitoring Officer. Authorising Officers must bring any suggestions for continuous improvement of this Document to the attention of the Monitoring Officer at the earliest possible opportunity.
5. In addition to the provisions in paragraph 4. the content of the policy will be reported to an appropriate committee annually, and when authorisations have been granted in any year, there will also be a report to the committee in respect of the operation of the policy no more than three months after the authorisation. The role of the committee is to oversee the RIPA policy and its proper application.
6. In terms of monitoring e-mails and internet usage, it is important to recognise the importance of the Council's e-mail and internet policies and guidance, the telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its Code of Practice on Employee Monitoring.
7. This policy only applies to the core functions of the Council, i.e the specific functions undertaken by the Council as opposed to the "ordinary" functions undertaken by all public authorities (for example employment issues, and contractual arrangements).

B. Council Policy Statement

1. The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Monitoring Officer, is duly authorised by the Council to keep this Document up to date and to amend, delete, add or substitute relevant provisions, as necessary.
2. This Policy requires:
 - (a) that all covert surveillance concerning the core public functions of the Council should comply with the requirements of RIPA;
 - (b) that only the Authorising Officers can properly authorise a covert surveillance exercise. Authorising Officers are those whose posts appear in Appendix 1 to this document; and

C. Authorising Officer Responsibilities

1. Any authorizations, renewals or cancellations must be made on and in accordance with the Forms provided in this Document. It is essential that Authorising Officers take personal responsibility for the effective and efficient operation of this Document.
2. It will be the responsibility of the Monitoring Officer to ensure that relevant members of staff are also suitably trained as 'Applicants' so as to avoid common mistakes appearing on Forms for RIPA authorisations.
3. Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Procedures Document and do not undertake or carry out any form of surveillance which is subject to the provisions of RIPA without first obtaining the relevant authorisations in compliance with this Document.
4. 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 an Authorising Officer approve any RIPA form unless, and until s/he is 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. If an Authorised Officer is in any doubt, s/he should obtain prior guidance on the same from the Council's Health & Safety Officer and/or the Monitoring Officer.
5. Authorising Officers must also ensure that, when sending copies of any Forms to the Monitoring Officer (or any other relevant authority), the same are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'.

D. General Information on RIPA

1. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their home and their correspondence, including certain aspects of business and professional life.
2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-
 - (a) **in accordance with the law;**
 - (b) **necessary** (as defined in this Document); **and**
 - (c) **proportionate** (as defined in this Document).
3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a '**covert human intelligence source**' ('CHIS') – e.g. undercover agents. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.
4. Directly employed Council staff and external agencies working for the Council are covered by the Act for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorising Officers. Authorising Officers are those whose posts appear in **Appendix 1** to this Document and, duly added to or substituted by the Monitoring Officer.
5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this Document and any further guidance that may be issued, from time to time, by the Monitoring Officer.
6. A flowchart of the procedures to be followed appears at **Appendix 2**.
7. The Monitoring Officer shall scrutinize authorizations to ensure that they contain all the necessary information and that they provide sufficiently robust evidence that the Authorizing Officer has properly applied the tests of necessity and proportionality.

E. What RIPA Does and Does Not Do

1. RIPA does:

- require prior authorisation of directed surveillance.
- prohibit the Council from carrying out intrusive surveillance.
- require authorisation of the conduct and use of a CHIS.
- require safeguards for the conduct and use of a CHIS.

2. RIPA does not:

- make unlawful conduct which is otherwise lawful.
- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

3. If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Monitoring Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

F. Types of Surveillance

1. **Surveillance'** includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- recording anything mentioned above in the course of authorised surveillance.
- surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

2. **Overt Surveillance**

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly.

3. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.

4. **Covert Surveillance**

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA).

5. RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

6. **Directed Surveillance**

Directed Surveillance is surveillance which:-

- is covert; and
- is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance);
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- it is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) of RIPA*).

7. *Private information* in relation to a person includes any information relating to his private and family life, his home, his correspondence and certain aspects of

business and professional life. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.
9. **For the avoidance of doubt, only those Officers designated and certified to be 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document are followed. If an Authorising Officer has not been 'certified' for the purposes of RIPA, s/he can NOT carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.**

10. ***Intrusive Surveillance***

This is when it:-

- is covert;
- relates to residential premises and private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

11. **This form of surveillance can be carried out only by police and other law enforcement agencies. Council Officers must not carry out intrusive surveillance.**

12. ***Confidential Information***

Particular care should be taken where the surveillance may disclose confidential information. This consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. Where it is likely that the surveillance will result in the acquisition of such information, only the Chief Executive or, in his absence, his nominated deputy, may grant authorization.

13. **Examples of different types of Surveillance**

Type of Surveillance	Examples
Overt	<ul style="list-style-type: none"> - Police Officer or Parks Warden on patrol - Signposted Town Centre CCTV cameras (in normal Use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	<ul style="list-style-type: none"> - CCTV cameras providing general traffic, crime or public safety information.
Directed must be RIPA authorised	<ul style="list-style-type: none"> - Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive – Council cannot do this!	<ul style="list-style-type: none"> - Planting a listening or other device (bug) in a person's home or in their private vehicle.

G. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of obtaining information; of covertly providing access to any information to another person or of covertly disclosing information obtained by, or as a consequence of the existence of, such a relationship.
2. RIPA does not 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.

What must be authorised?

3. The Conduct or Use of a CHIS require prior authorisation.
 - **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
 - **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.
4. **The Council can use CHIS's IF, AND ONLY IF, RIPA procedures, detailed in this Document are followed.**

Juvenile Sources

5. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. Only the Chief Executive, or in his absence, his nominated deputy, is duly authorised by the Council to use Juvenile Sources, as there are other onerous requirements for such matters.

Vulnerable Individuals

6. A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.
7. A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive or in his absence his nominated deputy, is duly authorised by the Council to use Vulnerable Individuals, as there are other onerous requirements for such matters.

Test Purchases

8. 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).

9. 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 also directed surveillance.

Anti-social behaviour activities (e.g. noise, violence, race etc)

10. 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.
11. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

H. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 2** provides a flow chart of process from application consideration to recording of information.

Authorising Officers

2. Forms can only be signed by Authorising Officers who have received training on RIPA. Authorising Officers should not authorise directed surveillance or the use of a CHIS in respect of any investigation in which they are involved. Authorised posts are listed in **Appendix 1**. This Appendix will be kept up to date by the Monitoring Officer
3. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire.
The authorisations do not lapse with time!

Training Records

4. Proper training will be given, or approved by the Monitoring Officer before Authorising Officers are certified to sign any RIPA Forms. A certificate of training will be provided to the individual and a Central Register of all those individuals who have undergone training or a one-to-one meeting with the Monitoring Officer on such matters will be kept by the Monitoring Officer.
5. If the Monitoring Officer feels that an Authorising Officer has not complied fully with the requirements of this Document, or the training provided to him, the Monitoring Officer is duly authorised to retract that Officer's certificate and authorisation until s/he has undertaken further approved training or a one-to-one meeting with the Monitoring Officer.

Application Forms

6. **'A Forms' (Directed Surveillance) – See Appendix 3**

Form A 1 **Application** for Authority for Directed Surveillance
Form A 2 **Renewal** of Directed Surveillance Authority
Form A 3 **Review** of Directed Surveillance Authority
Form A 4 **Cancellation** of Directed Surveillance

7. **'B Forms' (CHIS) – See Appendix 4**

Form B 1 **Application** for Authority for Conduct and Use of a CHIS
Form B 2 **Renewal** of Conduct and Use of a CHIS
Form B 3 **Review** of Conduct and Use of a CHIS
Form B 4 **Cancellation** of Conduct and Use of a CHIS

Grounds for Authorisation

8. Directed Surveillance (**A Forms**) or the Conduct and Use of the CHIS (**B Forms**) can be authorised by the Council only on one of the following grounds:-
- For the prevention or detection of crime or the prevention of disorder

Assessing the Application Form

9. Before an Authorising Officer signs a Form, **s/he must:-**
- (a) Be mindful of this Corporate Policy & Procedures Document, the Training provided by the Monitoring Officer and any other guidance issued, from time to time, by the Monitoring Officer on such matters;
 - (b) Satisfy his/herself that the RIPA authorisation is:-
 - (i) **in accordance with the law;**
 - (ii) **necessary** (i.e. that it is essential for the Prevention or detection of crime or disorder) in the circumstances of the particular case and is it necessary to use the covert technique requested; **and**
 - (iii) **proportionate** to what it seeks to achieve.
 - (c) In assessing whether or not the proposed surveillance is proportionate to the mischief under investigation consideration should be given to other appropriate means of gathering the information. **The least intrusive method will be considered proportionate by the courts.** When considering proportionality, regard should also be had to the following considerations:
 - (i) does the need for the activity outweigh the interference with privacy (consider the size and scope of the proposed activity against the gravity and extent of the perceived crime or disorder)?
 - (ii) is the proposed surveillance more extensive than reasonably necessary taking into account the degree of intrusion on the target and third parties? (consider whether there is another way of obtaining the information that involves less intrusive methods)
 - (iii) is the surveillance the only reasonable way of gaining the information? (identify what other methods have been considered and discounted)
 - (iv) What evidence of other methods considered and why these were not adopted.
 - (vi) The authorising officer must set out in his own words why the RIPA activity is necessary and proportionate having regard to the above tests and also the provenance of the information on which the application has been made.
 - (d) The authorising officer must record a clear description of what authority is being granted for and by reference to subjects, property or location and the type of surveillance permitted. This may not be the same as what is being requested.
 - (e) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far

as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

- (f) Set a date for review of the authorisation within one month of the grant and review on that date;
- (g) Obtain from the Monitoring Officer a Unique Reference Number (URN) for the application as follows:-
Year / Department / Number of Application.
Please note that only the Monitoring Officer or a person nominated by him can issue a reference number. An authorization will not be valid without this.
- (h) Ensure that any RIPA Departmental Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Monitoring Officer Central Register, **within 3 days of the relevant authorisation, review, renewal, cancellation or rejection**;
- (i) Take into account the likelihood of acquiring any confidential information including information concerning the physical or mental health or spiritual/religious counselling of a person, matters subject to legal privilege and confidential journalistic material.

Additional Safeguards when Authorising a CHIS

- 10. When authorising the conduct or use of a CHIS, the Authorising Officer **must also:-**
 - (a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;
 - (b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS in accordance with the Code of Practice for CHIS and Section 27 or 29 (5) of RIPA and this must address health and safety issues through a risk assessment;
 - (c) consider the likely degree of intrusion of all those potentially affected;
 - (d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained;
 - (e) ensure **records** contain particulars and are not available except on a need to know basis; and
 - (f) maintain records as per the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SJ 2000) 2725).

Urgent Authorisations

- 11. Urgent authorisations are not permitted.
Duration

12. The Form **must be reviewed in the time stated and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance, and for a maximum of 12 months (from authorisation) for a CHIS (after which time it ceases to have effect). However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the Forms do not expire!** The forms have to be reviewed and/or cancelled (once they are no longer required). The Authorising Officer should in any event seek regular updates on the investigation and a review should be undertaken prior to the designated time if there are any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in further intrusion into the private life of any person. The Authorising Officer may amend specific aspects of the authorisation upon a review, for example by discontinuing surveillance against particular persons or the use of particular tactics. Reviews and renewals should not broaden the scope of the investigation but can reduce its terms.
13. Authorisations can be renewed in writing before the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.
14. The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours.
15. When cancelling an authorisation, the authorising officer should;
 - (i) Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.
 - (ii) The reasons for the cancellation.
 - (iii) Ensure that surveillance equipment has been removed and returned.
 - (iv) Provide directions for the management of the product.
 - (v) Ensure details of the surveillance since the last review are properly recorded.
 - (vi) Record the value of the surveillance.

I. Working With / Through Other Agencies

1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this Document and the Forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.
2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc):-
 - (a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Monitoring Officer for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

- (b) wish to use the Council's premises for their own RIPA action, the Officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.
- (c) In terms of 2(a), if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

3. **If in doubt, please consult with the Monitoring Officer at the earliest opportunity.**

J. Record Management

1. **The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Monitoring Officer.**

2. ***Records maintained in the Service Area***

The following documents must be retained by the relevant Head of Service (or his/her designated Co-ordinator) for such purposes.

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN).

3. Each form will have a URN. The Monitoring Officer will issue the relevant URN to Applicants. The cross-referencing of each URN takes place within the Forms for audit purposes. The relevant service code to be followed is as per **Appendix 1**. Rejected Forms will also have URN's.

Central Register maintained by the Monitoring Officer

4. **Authorising Officers must forward details of each Form to the Monitoring Officer for the Central Register, within 3 days of the authorisation, review, renewal, cancellation or rejection. The Monitoring Officer will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary.**
5. The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations.

K. Role of the Monitoring Officer

- To ensure that authorized officers fully address the requirements of the authorization process, with particular emphasis on applying the tests of necessity and proportionality. The Monitoring Officer may instruct authorising officers to cancel authorisations that are not compliant with the requirements of RIPA.
- To provide guidance and training to authorized and applicant officers.
- To issue application numbers and maintain the Central Register of authorizations.

L. Concluding Remarks of the Monitoring Officer

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.
2. Obtaining an authorisation under RIPA and following this Document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.
3. Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must never sign or rubber stamp Form(s) without thinking about their personal and the Council's responsibilities.
4. Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.
5. For further advice and assistance on RIPA, please contact the Monitoring Officer. Details are provided on the front of this Document. If the Monitoring Officer is unavailable advice can be sought from an alternative Authorising Officer.

List of Authorising Officer Posts

Chief Executive
Head of Resources
Head of Planning and Environment
Head of Warwickshire County Council Internal Audit
Head of Business, Housing and Revenues
Head of Customer Access
Head of Technical Services

Service Codes for Use on Forms

CS	Corporate Support
PE	Planning and Environment
TS	Technical Services
CA	Customer Access
BEHR	Business Enterprise Housing and Revenues
R	Resources

IMPORTANT NOTES

- A.** Even if a post is identified in the above list the persons currently employed in such posts are not authorised to sign RIPA Forms (including a renewal or cancellation) unless s/he has been certified by the Monitoring Officer to do so.
- B.** Only the Chief Executive and the Monitoring Officer are authorised to sign Forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph **G** of this Document).
- C.** If in doubt, ask the Monitoring Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

RIPA FLOW CHART

APPENDIX 2

Requesting Office ('The Applicant') must:

- Read the Corporate Policy & Procedures Document and be aware of any other guidance issued by the Monitoring Officer.
- Determine that directed surveillance and/or a CHIS is required.
- Assess whether authorisation will be **in accordance with the law**.
- Assess whether authorisation is **necessary** under RIPA and whether it could be done overtly.
- Consider whether surveillance will be **proportionate**.
- If Authorisation is approved – review regularly.

If a less intrusive option is available and practicable
Use that option!

If authorisation is necessary and proportionate, prepare and submit an approved form to the Authorising Officer

Authorised officer must:

- Consider in detail whether all options have been duly considered, including the Corporate Policy & Procedures Document and any other guidance issued by the Monitoring Officer.
- Consider whether surveillance is considered by him/her to be necessary and proportionate.
- Authorise only if an overt or less intrusive option is not practicable.
- Set an appropriate review date (can be up to 3 months after authorisation date) and conduct the review.

The Applicant must:
REVIEW REGULARLY and **within one month of the grant of authorisation** (complete Review form) and

The Applicant must:
If operation is no longer necessary or proportionate, complete **CANCELLATION FORM** and submit to Authorised Officer.

ESSENTIAL
Send all Authorised (and any rejected) Forms, Review, Renewals and Cancellations to the Co-ordinator and to the Monitoring Officer within 1 week of the relevant event.

Authorised Officer must: if surveillance is still necessary and proportionate:

- Review Authorisation.
- Set an appropriate further review date.

Authorised Officer must:
Cancel authorisation when it is no longer necessary or proportionate to maintain the same.

NB: If in doubt, ask Monitoring Officer **BEFORE** any directed surveillance and/ Or CHIS is authorised, renewed, cancelled or rejected. Heads of Service will designate one of their Staff to be a Departmental Co-ordinator for the purpose of RIPA and advise the Monitoring Officer accordingly.

RIPA A FORMS: DIRECTED SURVEILLANCE

Form A1 : **Application** for authorisation to carry out directed surveillance.

Form A2 : Application for **Renewal** of Form A1.

Form A3 : **Review** of Form A1.

Form A4 : **Cancellation** of Form A1.

NB: If in doubt, ask Monitoring Officer BEFORE any directed surveillance and/or CHIS is authorised, cancelled or rejected.

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Unique Reference Number	
--------------------------------	--

Public Authority <i>(including full address)</i>			
Name of Applicant		Unit/Branch /Division	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

Unique Reference Number	
--------------------------------	--

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521.¹

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

¹ For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Unique Reference Number	
--------------------------------	--

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

Describe precautions you will take to minimise collateral intrusion.

Unique Reference Number	
--------------------------------	--

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

10. Confidential information [Code paragraphs 4.1 to 4.31].

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Unique Reference Number	
-------------------------	--

11. Applicant's Details

Name (print)		Tel No:	
Grade/Rank		Date	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?*]

13. Explain why you believe the directed surveillance is necessary [Code paragraph 3.3]. Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

Unique Reference Number	
--------------------------------	--

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

Date of first review	
-----------------------------	--

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review is known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		Grade / Rank	
Signature		Date and time	
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]			

Unique Reference Number	
-------------------------	--

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

--

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

--

Name (Print)		Grade/ Rank	
Signature		Date and Time	
Urgent authorisation Expiry date:		Expiry time:	
<i>Remember the 72 hour rule for urgent authorities – check Code of Practice.</i>	e.g. authorisation granted at 5pm on June 1 st expires 4.59pm on 4 th June		

**Part II of the
Regulation of Investigatory Powers Act 2000
Renewal of a Directed Surveillance Authorisation**

Unique Reference Number	
--------------------------------	--

Public Authority <i>(including full address)</i>	
--	--

Name of Applicant		Unit/Branch/ Division	
Full Address			
Contact Details			
Investigation/ Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	Date

Unique Reference Number	
--------------------------------	--

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

--

3. Detail the reasons why it is necessary to continue with the directed surveillance.

--

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

--

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

--

6. Give details of the results of the regular reviews of the investigation or operation.

--

Unique Reference Number	
--------------------------------	--

7. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

8. Authorising Officer's Comments. <u>This box must be completed.</u>

9. Authorising Officer's Statement.				
<p>I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing.</p> <p>This authorisation will be reviewed frequently to assess the need for the authorisation to continue.</p>				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">Name (Print)</td> <td style="width: 50%;">Grade / Rank - - - - -</td> </tr> <tr> <td>Signature - - - - -</td> <td>Date - - - - -</td> </tr> </table>	Name (Print)	Grade / Rank - - - - -	Signature - - - - -	Date - - - - -
Name (Print)	Grade / Rank - - - - -			
Signature - - - - -	Date - - - - -			
<table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">Renewal From:</td> <td style="width: 33%;">Time:</td> <td style="width: 33%;">Date:</td> </tr> </table>	Renewal From:	Time:	Date:	
Renewal From:	Time:	Date:		

Date of first review	
Date of subsequent reviews of this authorisation	

**Part II of the
Regulation of Investigatory Powers Act 2000**

Review of a Directed Surveillance Authorisation

Unique Reference Number	
--------------------------------	--

Public Authority <i>(including address)</i>	
---	--

Applicant		Unit/Branch/ Division	
------------------	--	----------------------------------	--

Full Address			
---------------------	--	--	--

Contact Details			
------------------------	--	--	--

Operation Name		Operation Number* <small>*Filing Ref</small>	
-----------------------	--	--	--

Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
--	--	---	--

Review Number	
----------------------	--

Details of review:

1. Review number and dates of any previous reviews.
--

Review Number	Date

Unique Reference Number	
--------------------------------	--

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.

--

3. Detail the reasons why it is necessary to continue with the directed surveillance.

--

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

--

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

--

Unique Reference Number	
--------------------------------	--

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

--

7. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

--

9. Authorising Officer's Statement.

I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Name (Print)	Grade / Rank	-----
Signature	-----	Date	-----

10. Date of next review.	
---------------------------------	--

**Part II of the
Regulation of Investigatory Powers Act 2000**

Cancellation of a Directed Surveillance authorisation

Unique Reference Number	
--------------------------------	--

Public Authority <i>(including full address)</i>	
--	--

Name of Applicant		Unit/Branch/ Division	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

Unique Reference Number	
--------------------------------	--

2. Explain the value of surveillance in the operation:

--

3. Authorising officer's statement.
--

I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.

Name (Print)	Grade
Signature	Date

4. Time and Date of when the authorising officer instructed the surveillance to cease.

Date:		Time:	
--------------	--	--------------	--

5. Authorisation cancelled.	Date:	Time:
------------------------------------	--------------	--------------

RIPA B FORMS : COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Additional Notes on CHIS (This is an extract from Home Office Code of Practice on CHIS)

MANAGEMENT OF SOURCES

Tasking

1. Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, 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.
2. The person referred to in section 29(5)(a) of the 2000 Act 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;
3. The person referred to in section 29(5)(b) of the 2000 Act will be responsible for the general oversight of the use of the source.
4. 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 Trading Standards 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 relevant public authority to determine where, and in what circumstances, such activity may require authorisation.
5. It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.
6. It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and re-authorised (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.

7. Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

8. Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each source.
9. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.
10. In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

11. Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. 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.
12. The person defined at section 29(5)(a) of the 2000 Act is responsible for bringing to the attention of the person defined at section 29(5)(b) of the 2000 Act any concerns about the personal circumstances of the source, insofar as they might affect:
 - the validity of the risk assessment
 - the conduct of the source, and
 - the safety and welfare of the source.
13. Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.
 - Form B1** : **Application** for authorisation of the **Use** or **Conduct** of a Covert Human Intelligence Source (CHIS).
 - Form B2** : Application for **Renewal** of Form B 1.
 - Form B3** : **Review** of Form B1.
 - Form B4** : **Cancellation** of Form B1

NB: If in doubt, ask the Monitoring Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
---	--

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)

Public Authority <i>(including full address)</i>			
Name of Applicant		Service/ Department/ Branch	
How will the source be referred to? i.e. what will be his/her pseudonym or reference number)?			
What is the name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare (often referred to as the Handler)?			
What is name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source (often referred to as the Controller)?			
Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source's true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?			
Investigation/Operation Name (if applicable)			

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
---	--

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. ² Where appropriate throughout amend references to the Order relevant to your authority.

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail the purpose for which the source will be tasked or used.

4. Describe in detail the proposed covert conduct of the source or how the source is to be used.

5. Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (eg. SI 2010 No. 521)

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

² For local authorities: The formal position of the authorising officer should be given. For example, Head of Trading Standards.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
---	--

6. Explain why this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 3.2]

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

Describe precautions you will take to minimise collateral intrusion and how any will be managed.

8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source? (see Code paragraphs 3.17 to 3.18)

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
---	--

9. Provide an assessment of the risk to the source in carrying out the proposed conduct. (see Code 6.14)

10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means? [Code paragraphs 3.3 to 3.5]

**11. Confidential information. [Code paragraphs 4.1 to 4.21]
Indicate the likelihood of acquiring any confidential information.**

References for any other linked authorisations:

12. Applicant's Details.

Name (print)		Grade/Rank/Position	
Signature		Tel No:	

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).

Date

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] The authorisation should identify the pseudonym or reference number of the source, not the true identity.

14. Explain why you believe the conduct or use of the source is necessary. [Code paragraph 3.2]

Explain why you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement. [Code paragraph 3.3 to 3.5]

15. (Confidential Information Authorisation.) Supply details demonstrating compliance with Code paragraphs 4.1 to 4.21

16. Date of first review:

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
---	--

17. Programme for subsequent reviews of this authorisation: [Code paragraphs 5.15 and 5.16]. Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.

--

18. Authorising Officer's Details

Name (Print)		Grade/Rank/Position	
Signature		Time and date granted*	
		Time and date authorisation ends	

** Remember, an authorisation must be granted for a 12 month period, i.e. 1700 hrs 4th June 2006 to 2359hrs 3 June 2007*

19. Urgent Authorisation [Code paragraphs 5.13 and 5.14]: Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

--

20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer

--

21. Authorising Officer of urgent authorisation

Name (Print)		Grade/Rank/Position	
Signature		Date and Time	
Urgent authorisation expiry date:		Expiry time:	

Remember the 72 hour rule for urgent authorisations – check Code of Practice [Code Paragraph 5.14]. e.g. authorisation granted at 1700 on 1st June 2006 expires 1659 on 4th June 2006

Unique Operation Reference Number* (*Filing Ref)	
---	--

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation

(Please attach the original authorisation)

Public Authority <i>(including full address)</i>	
--	--

Name of Applicant		Unit/Branch	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	Date

**Unique Operation Reference
Number*** (*Filing Ref)

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail why it is necessary to continue with the authorisation, including details of any tasking given to the source.

4. Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.

5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.

**Unique Operation Reference
Number*** (*Filing Ref)

6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source.

--

7. Detail the results of regular reviews of the use of the source.

--

8. Give details of the review of the risk assessment on the security and welfare of using the source.

--

9. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

10. Authorising Officer's Comments. This box must be completed.

--

Unique Operation Reference Number* (*Filing Ref)	
---	--

11. Authorising Officer's Statement. The authorisation should identify the pseudonym or reference number of the source not the true identity.

--

Name (Print)	Grade / Rank
---------------------------	---------------------

Signature	Date
------------------	-------------

Renewal From:	Time:	Date:
		End date/time of the authorisation

NB. Renewal takes effect at the time/date of the original authorisation would have ceased but for the renewal

Date of first review:	
Date of subsequent reviews of this authorisation:	

Unique Operation Reference Number* (*Filing Ref)	
---	--

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Review of a Covert Human Intelligence Source (CHIS) authorisation

Public Authority <i>(including full address)</i>	
--	--

Applicant		Unit/Branch	
------------------	--	--------------------	--

Full Address	
---------------------	--

Contact Details	
------------------------	--

Pseudonym or reference number of source	
--	--

Operation Name		Operation Number* <small>*Filing Ref</small>	
-----------------------	--	--	--

Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
--	--	---	--

Review Number	
----------------------	--

**Unique Operation Reference
Number*** (*Filing Ref)

Details of review:

1. Review number and dates of any previous reviews.

Review Number	Date

2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue with using a Covert Human Intelligence Source.

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

Unique Operation Reference Number* (*Filing Ref)	
---	--

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

--

7. Give details of the review of the risk assessment on the security and welfare of using the source.

--

8. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

9. Review Officer's Comments, including whether or not the use or conduct of the source should continue?

--

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

--

Name (Print) **Grade / Rank**

Signature **Date**

Date of next review:

--

Unique Operation Reference Number* (*Filing Ref)	
---	--

**Part II of the
Regulation of Investigatory Powers Act (RIPA)
2000**

**Cancellation of an authorisation for the use or conduct of
a Covert Human Intelligence Source**

Public Authority <i>(including full address)</i>	
--	--

Name of Applicant		Unit/Branch	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			

**Unique Operation Reference
Number*** (*Filing Ref)

--

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

--

2. Explain the value of the source in the operation:

--

3. Authorising officer's statement. This should identify the pseudonym or reference number of the source not the true identity.

--

Name (Print)	Grade
Signature	Date

4. Time and Date of when the authorising officer instructed the use of the source to cease.

Date:		Time:	
--------------	--	--------------	--