Wycombe District Council
The Regulation of Investigatory Powers Act 2000 (RIPA) Policy and Procedures

people place pounds
getting our priorities right

Current version:	**March 201**
Next review:	**March 2018**
Author:	**Catherine Herries-Smith**
	Principal Solicitor/Information Officer

CONTENTS PAGE

NB: The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within Wycombe District Council, this 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 Senior Responsible Officer (SRO). For the avoidance of doubt, therefore, all references to duly certified Authorising Officers refer to 'Designated Officers' under RIPA.

INTRODUCTION AND KEY MESSAGES

1. STATUS AND REVIEW OF COVERT SURVEILLANCE

1.1. This Policy is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA') and the Home Office's Revised Codes of Practice on 'Covert Surveillance and Property Interference' and 'Covert Human Intelligence Sources' (covert surveillance will be used only rarely and in exceptional circumstances) and the non-statutory Home Office Guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance (October 2012). Reports will be made regularly to the Audit Committee via the Cabinet Member for Performance and Finance. The Audit Committee will report any concerns to the Cabinet. An annual report will be made directly to the Cabinet and will concern RIPA policy and overall RIPA performance of the Council. Elected Members will not, however, be involved in decision making in individual cases, and should not receive details of individual cases or properties subject to surveillance (Code of Practice for Covert Surveillance (3:30)).

1.2. A Senior Responsible Officer (SRO), who is a member of the corporate leadership team, will have overall responsibility for RIPA within the Council, and will be responsible for ensuring the integrity of the process, compliance with RIPA, engagement with Office of Surveillance (OSC) Commissioners or Inspectors at Inspections and for overseeing the implementation of any recommendations made by an Inspection. In addition s/he is required to ensure the standard of Authorising Officers. This means that s/he exercises ultimate oversight over the RIPA process.

1.3. A RIPA Co-ordinating Officer (RCO) will be at the heart of day to day management of RIPA, with the SRO as the officer with overall responsibility. The RIPA Co-ordinating Officer should undertake four functions:

1.3.1 Maintenance of a Central Record of Authorisations and collation of all original RIPA documentation;

1.3.2 Day to day oversight of the RIPA process, particularly of the submitted documentation;

1.3.3 Organising corporate training for RIPA;

1.3.4 Raising RIPA awareness within the Council.

1.4. 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 RIPA Co-ordinating Officer, for advice and assistance. Appropriate training and development will be organised and training given to relevant Authorising Officers, other senior managers and all likely applicants.

1.5. All original RIPA authorization documentation will immediately following creation be passed to the RCO to be included within a Central Record. The Head of Environment, Head of Community Services and the Head of Finance shall retain copies of all RIPA authorisations, reviews, renewals, cancellations and rejections for their own services.

1.6. For any other service that may need to carry out surveillance the relevant Authorising Officer will be the Head Of Finance (for example Ad Hoc CCTV surveillance requests) and the relevant officers will need to ensure that agreement is sought before any surveillance is carried out. Original authorisations shall be passed to the RCO for inclusion on the Central Record and copies will be held within the Finance Division on an 'ad hoc' authorisations file.

1.7. 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. Such actions can only be carried out for the purposes of preventing crime and disorder.

1.8. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the Councils e-mail and internet policies and guidance and the Data Protection Act 1998. RIPA forms should be used where relevant and they will be only relevant where the criteria listed on the Forms are fully met.

1.9. If you are in any doubt on RIPA, this Document or the related legislative provisions, please consult the RIPA Co-ordinating Officer at the earliest possible opportunity.

POLICY

2. COUNCIL POLICY STATEMENT

2.1. 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.

2.2. The Council has resolved that:

- all covert surveillance exercises conducted by the Council should comply with the requirements of RIPA;
- only the named officers shall be permitted to authorise a covert surveillance exercise; and
- this Report will be referred to all those Advisory Teams which may carry out covert surveillance.

AUTHORISING OFFICER RESPONSIBILITIES

3. AUTHORISING OFFICER RESPONSIBILITIES

3.1. The Corporate Policy, Procedures and the Forms provided in this Document must be used for Covert Surveillance. Authorising Officers will take personal responsibility for the effective and efficient operation of this policy.

3.2. Authorising Officers will undertake suitable training on this policy and RIPA and be duly certified to take action under this Document.

3.3. It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'Applicants' so as to avoid common mistakes appearing on Forms for RIPA authorisations.

3.4. 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 without first obtaining the relevant authorisations in compliance with this Document.

3.5. 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, they are satisfied the health and safety of Council employees/agents is suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed.

3.6. If an Authorising Officer is in any doubt, they should obtain prior guidance on the same from the RIPA Co-ordinating Officer.

3.7. Authorising Officers should pass original authorization documentation to the RCO. They must also ensure that they keep copies of all necessary documentation to undertake any necessary reviews.

DEFINITIONS AND GENERAL INFORMATION

4. GENERAL INFORMATION ON RIPA

4.1. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedom 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 correspondence.

4.2. 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).

4.3. 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, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

4.4. At the start of an investigation, Council officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use it must be clear that the threshold is met and that it is necessary and proportionate to use it. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative or operational terms;

4.5. The authorization will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorized should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. An offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

4.6. The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing as far as reasonably practicable, what other methods had been considered and why they were not implemented.
- ensuring that the perceived crime or offence satisfies the crime threshold for Directed surveillance.

4.7. 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 Senior Responsible Officer.

4.8. 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 RIPA Co-ordinating Officer.

4.9. A flowchart of the procedures to be followed appears at Appendix 2 and below are links to Home Office and Office of Surveillance Commissioners Codes of Practice:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interrefernce_web__2_.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interrefernce_web__2_.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf

5. WHAT RIPA DOES AND DOES NOT DO

5.1. RIPA does:

- require prior authorisation and judicial approval 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.

5.2. 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 information from the Land Registry as to the ownership of a property.

5.3. If the Authorising Officer or any Applicant is in any doubt, they should ask the RIPA Co-ordinating Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

6. TYPES OF SURVEILLANCE

6.1. '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.

Overt Surveillance

6.2. 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 test purchases which do not give rise to a 'relationship' being established, and where no covert technical equipment is worn), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

6.3. 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 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.

Covert Surveillance

6.4. 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).

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

Directed Surveillance

6.6. Directed Surveillance is surveillance that is:-

- covert; and
- not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance);

- 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).

6.7. Private information in relation to a person includes any information relating to their private and family life, home and correspondence. 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 them and others that they come into contact, or associate, with.

6.8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, that involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs their business may also reveal information about their private life and the private lives of others.

6.9. Confidential information is information held in confidence relating to the physical or mental health or spiritual counseling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a legal adviser and client (covered by legal privilege), between health professional and a patient, or information from a patient's records. Only the CEO or his/her Deputy can authorize covert surveillance involving confidential information.

6.10. 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, they CANNOT carry out or approve/reject any action set out in this Policy.

6.11. Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a minimum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

6.12. Any covert operation in which confidential information might be required requires authorization by the Chief Executive or his/her Deputy.

Intrusive Surveillance

6.13. This is when surveillance:-

- 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.

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

Social Media

6.15. Where social media sites (SMS) are used for investigatory purposes officers should be mindful of Office of Surveillance Commissioners' 2014 Guidance. In particular, where access controls are applied the author is deemed to have a reasonable expectation of privacy. Where data is "open source" repeated viewing may constitute directed surveillance on a case by case basis and should be borne in mind. In addition, an authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a public authority or someone acting on its behalf (i.e. the activity is more than mere reading the site's content).

A member of the public authority should not adopt the identity of a person know, or likely to be known, to the subject of interest or users of the site without authorization, and without the consent (explicit) of the person whose identity is used, and without considering the protection of that person

Examples of types of Surveillance

6.16. Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	• 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.
Covert but not requiring prior authorisation	• CCTV cameras providing general traffic, crime or public safety information. • when conducted 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 authorization under Part II of the 2000 Act to be sought (i.e. an officer chances to observe conduct relevant to a criminal or law and order offence)
Directed must be RIPA authorised.	• 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. (Test purchases can also amount to a CHIS. Whether or not a 'relationship' exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity.)
Intrusive – Council cannot do this	• Planting a listening or other device (bug) in a person's home or in their private vehicle.

7. CONDUCT AND USE OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

Who is a CHIS?

7.1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping to obtain information.

7.2. 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?

7.3. Under the 2000 Act, a person is a CHIS if:

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

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

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. The Conduct or Use of a CHIS requires 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.

7.4. The Council can use CHIS's IF, AND ONLY IF, RIPA procedures, detailed in this Document are followed.

Juvenile Sources

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

Vulnerable Individuals

7.6. 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 themself, or unable to protect themself against significant harm or exploitation.

7.7. 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 or his/her Deputy is authorised by the Council to use Vulnerable Individuals, as there are other onerous requirements for such matters.

Test Purchases

7.8. In the context of CHIS, the word “establishes” when applied to a relationship means “set up”. It does not require, as “maintains” does, endurance over any particular period. For example, a relationship of seller and buyer may exist between a shopkeeper and a customer even if only a single transaction takes place: repetition is not necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time

of the contact between seller and buyer. There is no obligation to authorize as a CHIS everyone who is within the definition of a CHIS; this is matter for judgement according to all the circumstances of the case.

7.9. When an adult or young person, pursuant to an arrangement with an officer of a public authority, carries out a test purchase at a shop, he may be a CHIS. It does not follow that there must be a CHIS authorization because designated public authorities are empowered but not obliged to authorize a CHIS. But if covert equipment is worn by the test purchaser, or an adult is observing the test purchase, there can be no doubt that authorization for Directed Surveillance is required and such authorization must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person and desirable in relation to an adult.

Anti-Social Behaviour Activities (e.g. noise, violence, race etc)

7.10. 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.

7.11. Recording sound (with a DAT recorder or other similar device) 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. For the avoidance of doubt no machine should be used which pre or post records without the complainant being informed. This may otherwise constitute intrusive surveillance. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

PROCEDURES

8. AUTHORISATION PROCEDURES

8.1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

8.2. Appendix 2 provides a flow chart of process from application consideration to recording of information.

Authorising Officers

8.3. Forms can only be signed by Authorising Officers who hold a Certificate from the Senior Responsible Officer. Authorised posts are listed in Appendix 1. This Appendix will be kept up to date by the RIPA Co-ordinating Officer, and added to as needs require. The RIPA Co-ordinating Officer on the authority of the Senior Responsible Officer is duly authorised to add, delete or substitute posts listed in Appendix 1.

8.4. Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management. 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

8.5. Proper training will be given, or approved by the RIPA Co-ordinating 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 RIPA Co-ordinating Officer on such matters will be kept by the RIPA Co-ordinating Officer.

8.6. If the Senior Responsible Officer feels that an Authorising Officer has not complied fully with the requirements of this Document, or the training provided, the Senior Responsible Officer is duly authorised to retract that Officer's certificate and authorisation until they have undertaken further approved training or a one-to-one meeting with the RIPA Co-ordinating Officer.

Application Forms

8.7. Only the approved RIPA forms set out in this Document must be used. Any other forms used will be rejected by the Authorising Officer and/or the RIPA Co-ordinating Officer. To assist an Authorising Officer to reach a proper judgement the provenance of data, information or intelligence on which the application is made should be clear.

8.8. '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

8.9. '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

8.10. Directed Surveillance (A Forms) or the Conduct and Use of the CHIS (B Forms) can be authorised by the Council only one of ground:-

- For the prevention or detection of crime or of preventing disorder. Local authorities can only authorise the use of directed surveillance under RIPA to prevent or detect criminal offences that are punishable whether on summary conviction or indictment by a minimum term of at least 6 months' imprisonment or are related to the underage sale of alcohol or tobacco.

Assessing the Application Form

8.11. Before an Authorising Officer signs a Form, they must:-

(a) Be mindful of this Policy & Procedures Document, the Training provided externally or by the RIPA Co-ordinating Officer and any other guidance issued, from time to time, by the RIPA Co-ordinating Officer on such matters;

(b) Satisfy themself that the RIPA authorisation is:-

(i) in accordance with the law;

(ii) necessary in the circumstances of the particular case on one of the grounds mentioned in paragraph 8.10 above; and

(iii) proportionate to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. The use of a source should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

(d) 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;

(e) Set a date for review of the authorisation and review on only that date;

(f) All authorizations should be cancelled before their expiry date unless subject to renewal;

(g) All original RIPA documentation should be submitted to the RIPA Co-ordinating Officer to enter details on a Central Record of authorizations, allocating a Unique Reference Number (URN) for the application, with copies being retained in the applying Business Unit.

(h) In order that the authorisation meets the crime threshold for judicial approval the Authorising Officer must be satisfied that the requisite crime threshold is satisfied. Examples of cases where the offence being investigated attracts a minimum custodial sentence of 6 months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.

Additional Safeguards when Authorising a CHIS

8.12. 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 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; and

(e) ensure records contain particulars and are not available except on a need to know basis.

Urgent Authorisations

8.13

8.13. The power to make urgent oral authorisations has been removed, because section 43(1)(a) of RIPA no longer applies to authorisations requiring a magistrate's approval. All authorisations, even if urgent, must be made in writing.

Duration

8.14. 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 3 months (from authorization unless cancelled) for Directed Surveillance, and 12 months (from authorisation) for a CHIS. In both cases renewals must be granted before an authorization expires.

8.15. 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). On Cancellation forms, Authorising Officers should provide directions for where and how the intelligence/evidence gleaned will be stored and managed.

8.16. 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.

8.17. The renewal will begin on the day when the authorisation would have expired. If during an investigation which has been authorized it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the crime threshold the use of directed surveillance should cease. If a directed surveillance authorisation is in force it should be cancelled.

Judicial approval

8.18. From 1 November 2012 a local authority who wishes to authorise the use of directed surveillance, acquisition of communications data and the use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorization or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate s/he will issue an order approving the grant or renewal for the use of the technique as described in the application. The flowchart at Appendix 5 outlines the procedure for applying for judicial approval

8.19. Following approval by the Authorising Officer the first stage of the process is for the investigating officer to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the Magistrates' Court to arrange a hearing. The Office of Surveillance Commissioners considers that the best officer to apply to the magistrate for approval of directed surveillance or CHIS is the Authorising Officer, though they recognize that this is not always practicable. Only s/he can

answer questions about his/her reasoning on necessity, proportionality, collateral intrusion and risk. The relevant Officer will provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon.

8.20. The original RIPA authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' office and in the event of any legal challenge or investigation by the Investigatory Powers Tribunal (IPT). The Court may wish to take a copy. In addition, the Investigating Officer will provide the JP with a partially completed Judicial application/order (at Appendix 5).

8.21. The order section of this form will be completed by the JP and will be the official record of the JP's decision. The relevant Officer will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and the Council will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

8.22. On the rare occasions where out of hours access to a JP is required local arrangements should be made with the relevant HMCTS staff. In these cases the Investigating Officer will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The Council should provide the Court with a copy of the signed judicial application/order form the next working day.

8.23. The hearing is a legal proceeding and therefore local authority officers need to be formally designated under standing orders (under s.223 Local Government Act 1972) to appear, be sworn in and present evidence or provide information as required by the JP.

8.24. The hearing will be conducted in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application. S/he may have questions to clarify parts, or require additional assistance.

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

8.26. Following their consideration of the case the JP will complete the order section of the Judicial application/order form recording their decision. The JP may decide to 1) approve the grant or renewal of an authorisation or notice, 2) refuse to approve

the grant or renewal of an authorisation or notice or 3) refuse to approve the grant or renewal and quash the authorisation or notice.

8.27. There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee. A local authority may only appeal a JP decision on a point of law by judicial review.

9. WORKING WITH / THROUGH OTHER AGENCIES

9.1. 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.

9.2. 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, they must obtain a copy of that agency's RIPA form for the record (a copy of which must be put on the Central Record of Authorisations);

(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.

9.3. In terms of 9.2 (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.

9.4. If in doubt, please consult with the RIPA Co-ordinating Officer at the earliest opportunity.

10. RECORD MANAGEMENT

10.1. The Council's Central Register of all authorisation forms will be maintained by the RIPA Co-ordinating Officer with the support of the PA to the Head if Democratic, Legal and Policy Services.

Records maintained in the Department

10.2. The following original documents must be passed to the RIPA Co-ordinating Officer immediately to retain and record details on a Central Record of Authorisations:

- the original Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record must include reference to all covert activities authorized by an 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;
- details of any magistrate's approval under s.32(a) of RIPA.

10.3. Each form will have a URN. The Departmental Co-ordinators will retain copies of original documents in connection with any authorisation.

Central Register maintained by RIPA Co-ordinating Officer but delegated to PA to Head of Democratic, Legal and Policy Services.

10.4. Authorising Officers must forward details of each Form to the RIPA Co-ordinating Officer immediately following creation of any authorisation, review, renewal, cancellation or rejection for the Central Record of Authorisations. The RIPA Co-ordinating Officer will monitor these and give appropriate guidance, from time to time, or amend this Document, as necessary.

10.5. 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.

CONCLUSION

11. CONCLUDING REMARKS

11.1. 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.

11.2. 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.

11.3. 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.

11.4. 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.

11.5. For further advice and assistance on RIPA, please contact the RIPA Co-ordinating Officer.

Version March 2017