REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

CORPORATE POLICY AND PROCEDURAL GUIDANCE DOCUMENT

Ann Maria Brown
Head of Legal and Democratic Services
Monitoring Officer
Crawley Borough Council

Town Hall
The Boulevard
Crawley
West Sussex
RH10 1UZ

Tel: 01293 438292
Fax: 01293 511803
Email: ann-maria.brown@crawley.gov.uk
Version Date: November 2016

References

Regulation of Investigatory Powers Act 2000 (RIPA) *as amended by RIPA 2010 and the* ***Protection of*** *Freedoms Act 2012*

Covert Surveillance Code of Practice Pursuant to Section 71 of the Regulations of Investigatory Powers Act 2000 *as amended by RIPA 2010*

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

Covert Human Intelligence Sources Code of Practice Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000 as amended by RIPA 2010

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

Home Office Guidance to Local Authorities in England and Wales on the judicial approval process for RIPA

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

Home Office Guidance for Magistrates Courts in England and Wales for a Local Authority application seeking an order approving the grant or renewal of a RIPA Authorisation or notice

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118174/magistrates-courts-eng-wales.pdf

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Amendment Order 2012

http://www.legislation.gov.uk/uksi/2012/1500/article/2/made

OGC Procedures and Guidance July 2016

https://osc.independent.gov.uk/wp-content/uploads/2016/07/OSC-Procedures-Guidance-July-2016.pdf

The Criminal Procedure and Investigations Act 1996 (CPIA)

The Police and Criminal Evidence Act 1984

The European Convention on Human Rights, **Human Rights Act 1998**

See also; Office of Surveillance Commissioners

http://www.surveillancecommissioners.gov.uk

CRAWLEY BOROUGH COUNCIL

CORPORATE POLICY AND PROCEDURAL GUIDANCE DOCUMENT

(REGULATION OF INVESTIGATORY POWERS ACT 2000) *AS AMENDED BY RIPA 2010 AND THE PROTECTION OF FREEDOMS ACT 2012 (RIPA)*

1. Introduction

1.1. This Corporate Policy and Procedures Document addresses the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) the revised Home Office's Codes of Practices in relation to the Covert Surveillance of Individuals, the use of Covert Human Intelligence Sources (CHIS), including undercover officer / agents / informants (Under Part ll of RIPA) and the changes to RIPA introduced by the **Protection of** Freedoms Act 2012

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

Crawley Borough Council takes the responsibility for ensuring that the RIPA procedures are continuously improved.

These procedures provide a summary and overview of the legislation and Codes of Practice. It is intended as a quick reference for Officers designated to authorise activities under RIPA. DO NOT seek to rely on them alone. In the event of any doubt, the officer should refer to the relevant legislation or Codes of Practice. Any Officer who is unsure about any aspect of this document should contact at the earliest opportunity the Council's Head of Legal and Democratic Services for advice and assistance. Appropriate Training and Development will be organised to relevant authorised officers and other senior officers.

1.2 Copies of this Document and Related Forms can be found on the Council's Intranet under Corporate Procedures.

1.3 The Head of Legal and Democratic Services will maintain and check The Corporate Central Register of all RIPA authorisations, Magistrates' approvals, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorised Officer however, to ensure that the Head of Legal and Democratic Services receives a copy of the relevant Forms within 1 week of authorisation, review renewal, cancellation or rejection.

1.4 RIPA and this Guidance Document is important for the effective and efficient operation of the enforcement with regard to Covert Surveillance and Covert Human Intelligence Sources. This document will therefore be kept under review by the Head of Legal and Democratic Services ~~a~~ in light of changes in legislation, case law**,** Guidance or for the continuous improvement of this Policy Document. **Reports will also be submitted to the Council's Committee who has responsibility for RIPA.**

1.5 Staff should, therefore, familiarise themselves with this document, RIPA and the Home Office's Codes of Practices. If you are in any doubt on RIPA, this Document or The Codes of Practices before undertaking any enforcement activities please consult The Head of Legal and Democratic Services at the earliest possible opportunity.

1.6 Officers must appreciate that should they fail to follow the requirement of the Act and Codes of Practices, Crawley Borough Council may be liable to claims alleging breaches of an individual's rights under the Human Rights Act 1998. Authorisation of operations as defined by RIPA can be looked upon is an insurance policy. A properly authorised operation can protect the Council from such claims. Each case must be considered on its own merits. If the operation:

- Involves Covert methods, and
- Includes the use of Surveillance, and
- There is a likelihood (not just the intention) of Private Information (about anyone) being obtained then it is highly likely that the operation needs to be authorised.

1.7 Failure to follow the Act and Codes may also adversely effect the admissibility of any evidence obtained using methods covered by the Act. The safety of members of the public supplying information to the council may also be compromised. When an authorisation is not in place it may not be possible to seek exemption from disclosure under the provisions of Public Interest Immunity.

1.8 When undertaking any covert investigation, officers should have regard to the health and safety of persons affected by the activity. This may include themselves, colleagues and members of the public. A risk assessment of the investigation technique being proposed should be undertaken, having regard to the Crawley Borough Council Statement of Policy on Health, Safety and Welfare and any supplemental guidance issued by individual departments.

1.9 The monitoring of internet and e-mail use is regulated by **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.** Logs of access to the Internet and use of e-mail are maintained by the Information Communications and Technology Division of The Resources Directorate. **The Council's Internet and Email Usage Policy does inform employees that internet and email usage may be monitored.**

1.10 **The Regulation of Investigatory Powers (Communications Data) Order 2003 (as amended)** which came into force on 5th January 2004 deals with Communications Data and applies to Local Authorities. The Order, together with accompanying Code of Practice allows Local Authorities to access Communications Data but only for the purpose of prevention or detection of crime.

2. Objective

2.1 The objective of this document is to ensure that all Covert Surveillance carried out by Council employees and that all Covert Human Intelligence Sources are used in accordance with the law. When carrying out such surveillance or using such sources, officers should also bear in mind the revised Codes of Practices issued by the Home Office.

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

and

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

Hard copies of both Codes of Practice have been circulated to Heads of Service and relevant staff.

3. Scope

3.1 This Corporate Policy and Procedural Guidance Document applies in all cases where "Directed Covert Surveillance" is being planned or carried out and a "Covert Human Intelligence Source" (CHIS) is used or planned to be used.

4. Does RIPA and this Policy apply to me?

4.1 The likely answer is "yes", if you undertake any form of surveillance of individuals or organisations in the conduct of your duties e.g. as part of the investigatory, enforcement or regulatory functions of the Authority.

4.2 The table below gives some examples of the types of functions in which surveillance work may be undertaken.

Examples of Covert Surveillance undertaken by local authority investigators are:

- Undertaking investigations into allegations of internal fraud may require surveillance activity.
- Observing persons suspected of Housing Benefit Fraud to see if they are going to and from a place of work.
- Training of a CCTV camera onto a particular trading premises to establish who opens and closes the premises each day.
- Enforcing of controls, planning / building regulations.

The above list is not exhaustive but it is illustrative of the types of activities that local authority investigators engage in and which would be classified as "Directed Surveillance" (see Section 5 for Definitions).

If in doubt as to whether this Policy and Guidance applies to your area of operation, it is better to ask rather than open the Authority and yourself to the consequences of non-compliance, as detailed in paragraphs 1.6, 1.7 and 4.4.

4.3 Reference should be made to section 80(c) of RIPA 2000. The effect of this paragraph is that enforcement duties should continue to be carried out by implication where surveillance takes place in circumstances where the conduct may not be authorised under the Act. General observation forms part of duties of the many law enforcement officers within a public authority and is not usually regulated by the 2000 Act. This covers to a large extent Local Authority enforcement powers and duties i.e. those activities which are carried out overtly e.g. Community Warden on patrol, unannounced inspections by Environmental Health and Enforcement Officers. Such observations may involve the use of equipment to merely reinforce normal sensory perception such as binoculars or the use of cameras, where this does not involve systematic surveillance of an individual.

4.3 Before any authorisation takes place officers must consider whether the surveillance falls under RIPA. Consideration needs to be given to the changes introduced by the Protection of Freedoms Act 2012 and also to circumstances when guidance suggest that RIPA does not apply.

4.4 The Code of Practice on Covert Surveillance 2014 at pages 18-25 outlines those circumstances when a RIPA authorisation is not required or not appropriate.

4.5 Examples include the following:

(a) The use of CCTV cameras and ANPR systems by public authorities do not usually require RIPA authorisation as they are generally carrying out overt rather than covert surveillance.

(b) If surveillance takes place as an immediate response to events, authorisation will not be required even if the surveillance would generally fall into one of the

categories of surveillance covered by RIPA.

Example 1
Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of public authorities and the obtaining of private information is unlikely.
A directed surveillance authorisation need not be sought.

Example 2
Overt surveillance equipment, such as town centre CCTV systems or ANPR, is used to gather information as part of a reactive operation (e.g. to identify individuals who have committed criminal damage after the event). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation

4.6 If the type of surveillance being considered does not fall under RIPA, an authorisation will not be required.

4.7 Even if RIPA does not apply, use of surveillance will still have to be in accordance with the Human Rights Act 1998 and will therefore need to be:

(a) Proportionate
(b) Necessary
(c) Non-discriminatory
(d) Lawful

4.8 **If you undertake surveillance in any form and do not follow the procedures as set out in this Policy and Guidance, then the consequences can be:**

A risk that, if surveillance is not conducted properly, the evidence obtained may be held to be inadmissible. The may result in the loss of a case e.g. at Court/Employment Tribunal/an Internal Disciplinary Hearing.

The Council could be exposed to a claim for compensation for a breach of Article 8 of the European Convention on Human Rights or a complaint to the Local Government Ombudsman or a referral to a RIPA Tribunal, along with any resulting adverse publicity.

The Office of Surveillance Commissioners conducts regular audits on how local authorities implement RIPA. If it is found that a local authority is not implementing RIPA properly then this could result in censure.

Failure to comply with this Policy and Guidance may be a disciplinary offence.

To avoid any issues of non-compliance, it is essential that this Policy and Guidance are followed. In the event of any uncertainty, it is better to ask than to fall foul of the Legislation.

5. General Information on RIPA

5.1 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 Crawley Borough Council, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his home and his correspondence.

5.2 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 rights 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).

5.3 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 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 balance.

5.4 A RIPA flowchart appears at **Appendix 2**

6. Definitions

6.1 **Authorising Officer.**
Means the person(s) designated under Sections 28 and 29 of the Act to grant authorisations for directed surveillance and the use and conduct of a Covert Human Intelligence Source, respectively. Within each department, such officers should be documented and be in accordance with **The Regulation of Investigatory Powers Act** (**Directed Surveillance and Covert Human Intelligence Sources**) **Order *2010*** *to Directors, Heads of Service, or equivalent.*

6.2 **Confidential Material.**
This includes: Matters of legal privilege; Confidential personal information (e.g. medical records); Confidential journalistic material.

Matters Subject to Legal Privilege. Includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client , made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege.

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

6.3 **Covert Human Intelligence Sources (CHIS).**
Commonly known as Agents, Informants, Undercover Officers it is the use or conduct of someone who establishes or maintains a personal or other relationship (this must be a relationship and not a conversation) with a person for the covert purpose of obtaining information.

6.4 **Covert Surveillance.**
Means surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place **(Section 26(9)(a) of RIPA)**. It can be either Directed or Intrusive.

6.5 **Directed Surveillance.**
Is surveillance which is covert but not intrusive and which is undertaken for the purpose of a specific investigation or specific operation in such a manner as is likely to result in obtaining private information about an individual (whether or not that person is specifically targeted for purposes of an investigation **(Section 26(10) of RIPA)**.

6.6 **Intrusive Surveillance.**
(Local Authorities have no power to grant authorisations for intrusive surveillance but it is included here to alert Officers to be aware of inadvertently breaching this rule)

Means covert surveillance carried out in relation to anything taking place on residential premises or in a private vehicle. This kind of surveillance may take place by means of either a person or device located inside residential premises or a private vehicle of the person who is subject to the surveillance or by means of a device placed outside which consistently provides a product of equivalent quality and detail as a product which would be obtained from a device located inside. **Local authorities are not authorised to conduct Intrusive Surveillance without the consent of the SOS.**

6.7 **Private Information.**
In relation to a person this includes any information relating to his/her private or family life, his home and his correspondence. It is important to remember that the Act is drafted in terms of the likelihood of obtaining private information rather than the intention to obtain it or about specific persons. Judgements from The European Court on Human Rights have concluded that private information indicates what happens in the home, family and private life but excludes business and commercial activities in the broad sense it includes the way the family conducts its affairs.

6.8 **Controller.**
Means the person or designated managerial officer responsible for overseeing the use of the source.

6.9 **Handler.**
an investigating officer having day to day responsibility for:

- Dealing with the source on behalf of the authority
- Directing the day to day activities of the source
- Recording the information supplied by the source
- Monitoring the security and welfare of the source

6.10 **Conduct of a Source.**
Any action of that source, falling within the terms of the Act, or action incidental to it (i.e. What they do).

6.11 **"The Use" of a Source.**
Any action to induce, ask or assist a person engaged in the conduct of a source or to obtain information by means of an action of the source (i.e. What they are asked to do).

Residential Premises Means any **premises** occupied by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation), but does not include common areas to such premises, **front gardens or driveways visible to the public.**

Premises can also include any vehicle or moveable structure used within the definition above.

Private Vehicle Means any vehicle which is used primarily for private purposes of the person who owns it, or otherwise has a right to use it, but would not include any person whose right to use the vehicle arises from making payment for a particular journey.

Vehicle also includes any vessel, aircraft or hovercraft.

6.12 **Surveillance includes: (Section 48(2))**

- Monitoring, observing or listening to persons, watching or following their movements, their conversations, or other such activities or communications.

- Recording anything monitored, observed or listened to in the course of authorised

surveillance.

- Surveillance by or with the assistance of a surveillance device (any apparatus designed or adapted for use in surveillance).

6.13 **Surveillance does not include: (Section 48(3))**

(a) any conduct of a Covert Human Intelligence Source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source;

(b) the use of a Covert Human Intelligence Source for so obtaining or recording information; or
(c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorised under –

(i) section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services); or
(ii) Part lll of the Police Act 1997 (powers of the police and of custom officers).

6.14 Examples of different types of Surveillance:

Type of Surveillance	**Examples**
<u>Overt</u>	- Police Officer or Community 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.)
<u>Covert</u> but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information.
<u>Directed</u> must be RIPA authorised.	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit.
	- 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.
<u>Intrusive - Crawley Borough Council cannot do this</u> unless consent is obtained from S.O.S	- Planting a listening or other device (bug) in a person's home or in their private vehicle.

7. Covert Surveillance

<u>What is Covert Surveillance</u>

7.1 Covert Surveillance means **surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place**. Covert Surveillance within the meaning of the act falls into two categories Directed and Intrusive (please see Definitions Section).

Each operation needs to be examined to decide whether or not the surveillance is overt or covert. Two examples are:

- Enforcement of Private Hire licensing. If a licensing officer flags down a Private Hire vehicle and identifies him/herself to the driver when it stops then that is overt. On the other hand, riding as a passenger before making the identification would be covert.

- Use of a mobile CCTV camera to cover a blind spot in an area where fixed CCTV cameras are in use may be covert unless signage specific to the mobile camera is also put in place, even though the mobile camera may be in view rather than hidden.

7.2 On occasion planned surveillance may be undertaken which is not covert. However, each operation must be assessed on its merits to decide whether or not authorisation is required. On the face of it, an operation may appear to be not covert or not directed but may, in fact, need to be authorised. Whether or not surveillance is **directed** may depend on how narrow the target area is. The target does not have to be specified – RIPA is drafted in terms of the likelihood of obtaining private information rather than the intention to obtain it or about specific persons.

7.3 RIPA provides that surveillance will be lawful if an authorisation for such surveillance has been properly issued and a person acts in accordance with that authorisation.

7.4 An Authorisation provides lawful authority for a Public Authority to carry out Directed Surveillance.

7.5 Relevant Directors/Heads of Services should maintain a Register of all authorisations, Magistrate approvals, renewals, reviews, cancellations and rejections this information is also maintained in the Central Register held within the Legal and Democratic Services Division of the Chief Executive's Directorate. Where possible, Authorising Officers should not authorise operations in which they are directly involved.

Whenever surveillance takes place and is for the purpose of obtaining, or is likely to obtain, private information about a person (whether or not they are the target of the operation) an authorisation should be obtained.

7.6 By obtaining an authorisation, the surveillance operation, is carried out in accordance with the law and the safeguards that exist.

7.7 Prior to granting an authorisation the Authorising Officer must be satisfied that the proposed surveillance is necessary on specific grounds and is proportionate to what it seeks to achieve.

7.8 Before applying for an authorisation, the Investigating Officer should consider whether or not the evidence sought could be obtained by alternative methods.

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

Who is a CHIS?

A CHIS is a person who establishes or maintains a personal relationship or other relationship with a person in order to covertly obtain or disclose information. In a local authority, a CHIS is restricted to an informant or an officer working under cover.

A CHIS would not be:

- A member of the public who volunteers information to the local authority, such as a person who complains that they purchased food passed its use by date from their local supermarket. In that case the relationship between customer and provider is too remote. However, if the information were to be provided by an employee of the supermarket who was alleging that the food was being sold passed its use by date, then such a person *would be* a CHIS as a relationship exists namely one of employer/employee.

- An officer who merely goes into a shop and purchases an item without engaging in dialogue except for "how much"? and "thank you" , would not be a CHIS as, although the officer is working under cover, the officer is not seeking information from that person or to gain that person's trust.

- An officer who attends premises and identifies him/herself and then either carries out a statutory inspection or has entered in pursuance of a warrant of entry issued by a court, is not a CHIS. There is nothing covert about their visit.

What must be authorised?

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 including asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

8.1 **An Authorising Officer should not grant an authorisation** for use of a CHIS unless they are satisfied of the following:-

- That at all times there will be an officer who will have day to day responsibility for dealing with the source on behalf of the Council and for the source's security and welfare.

- That at all times there will be another officer (senior to the officer having responsibility under bullet point 1 above) who will have general oversight of the use made of the source.

- That at all times there will be an officer responsible for maintaining a record of the use made of the source, and

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

8.2 It should be considered that the information may well be given secretly and may not be revealed to the defendant as it may well be deemed to be sensitive in accordance with the Criminal Procedures and Investigations Act 1996. It should also be borne in mind that an informant may well be providing regular information during an investigation whereas a member of the public complaining may well be doing so as a one off.

8.3 **Safety and Welfare of a CHIS**

The safety and welfare of the source and foreseeable consequences to others should be taken into account in deciding whether or not to grant an authorisation. A risk assessment

determining the risk to the source in acting as a source of information to the Council and in particular, identifying and assessing the risks should the identity of the source become known, should be carried out. The welfare and security of the source after operations have ceased should be considered at the outset. The officer having responsibility under Paragraph 8.1 above (i.e. the officer with day to day responsibility for the source) should report to the officer having general oversight 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

The officer having responsibility under paragraph 7.1 can also be a CHIS and their health and safety should not be overlooked. If officers are to be used as a CHIS, the arrangements mentioned above should be followed so that the source is correctly managed.

8.4 **Juvenile Sources**

Special safeguards apply to the use or conduct of Juvenile sources (i.e. under 18 years old). Authorising Officers should abide by The Home Office Code of Conduct relating to Juveniles.

8.5 **Vulnerable Individuals**

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 maybe unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

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

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.

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.

How is an Application for a CHIS authorisation made?

An application for authorisation for a Covert Human Intelligence Source (CHIS) must be made in writing. It will specify:

- The reasons why the authorisation is necessary in the particular case and the grounds listed in the Act;
- The necessity of the authorisation in the particular case concerned;
- The reasons why the authorisation is considered proportionate to what it seeks to achieve;
- The purpose for which the source will be tasked or deployed;

- Where a specific investigation or operation is involved, the nature of that investigation or operation;
- The nature of what the source will be tasked to do;
- The level of authority required;
- The details of any potential collateral inclusion and why the intrusion is justified;
- Details of the risk assessment undertaken on the security and welfare of using the source; and
- The details of any confidential information that is likely to be obtained as a consequence of the authorisation.

The application for a **CHIS** Authorisation will be made on the approved RIPA Forms **(Appendix 4**).These forms can be found on the Home Office web site using the following links:

Form 4:1 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application?view=Binary
Application of the use of a Covert Human Intelligence Source (CHIS)

Form 4:2 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review?view=Binary
Reviewing the use of Covert Human Intelligence Source (CHIS)

Form 4:3 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal?view=Binary
Renewal of authorisation to use Covert Human Intelligence Source (CHIS)

Form 4:4 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation?view=Binary
Cancellation of Covert Human Intelligence Source (CHIS)

9. General Rules on Authorisations

Need for Authorisation

9.1 Obtaining appropriate authorisation for surveillance will be of importance to ensure that any evidence obtained is not to be judged inadmissible in any subsequent legal proceedings, as well as to provide the Council with some protection if the surveillance activities of its officers are ever challenged under the Human Rights Act, as part of a Judicial Review of a Council decision or in any referral to the Ombudsman.

9.2 Whenever it is proposed to conduct Directed Surveillance, an authorisation should be sought under RIPA as set out in the following paragraphs.

The Application Forms for Directed Surveillance can be found in **Appendix 3** The forms are located under RIPA Part ll Standard Forms Directed Surveillance and can be found on the Home Office web site using the following links

Form 3.1 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc?view=Binary
Application for the use of Directed Surveillance

Form 3:2 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/review-

directed-surveillance?view=Binary
Review of the use of Directed Surveillance

Form 3:3 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/renewal-directed-surveillance?view=Binary
Renewal of Directed Surveillance

Form 3:4 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan?view=Binary
Cancellation of the use of Directed Surveillance

9.3 **Authorisation**

a) Before an Authorised Officer signs a form he or she must be mindful of this Corporate Policy and Procedures Document, any training that has been provided and any other guidance issued from time to time by Head of Legal and Democratic Services. An authorisation *should not* be granted unless the Covert Surveillance/use of CHIS is:-

i. In accordance with the law

ii. Necessary in the circumstances of the particular case

iii. Proportionate to what it seeks to achieve

Necessary and Proportionate

9.4 **In terms of necessary:**
For interference with an individuals Rights under Article 8 of the ECHR to be necessary the Covert surveillance/use of CHIS **must** be pursuant to the following ground:-

For the purpose of preventing or detecting crime.

Note: The criminal offence which it is sought to be prevented or detected must be punishable by a maximum term of at least 6 months imprisonment or would constitute an offence under Sections 146, 147 of 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence sources) Order 2010.

It is important that officers address the question why surveillance is necessary in this particular case, in that the desired information cannot reasonably be acquired by overt means.

In terms of **proportionate:**

Even if the proposed activity is considered to be necessary, the person considering the application for authorisation must consider whether the activities are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. This element is designed to ensure that the proposed course of action does not represent a sledge hammer being used to crack a walnut. The activity **will not be proportionate** if:

- The intrusiveness is excessive in relation to the value of the information to be obtained, or

- The information sought could be obtained by less intrusive means.

The least intrusive method will be considered proportionate by the Courts

Collateral Intrusion

The officer seeking the authorisation should also consider the possibility of COLLATERAL INTRUSION. This is where interference with the privacy of others not subject to the original surveillance may occur. Collateral Intrusion might occur if equipment used records information not sought. An example is in Noise Monitoring where it may be inappropriate to place a recording device adjacent to a bedroom wall. Steps should be taken to assess the risk and, where possible, reduce the risk of collateral intrusion. Where unforeseen collateral intrusion occurs during an operation the Authorising Officer must be notified and consideration given to amending the authorisation following a review. Measures must be taken whenever practicable to avoid or minimise so far as is possible Collateral Intrusion an aspect the matter maybe of determining proportionality.

Consideration must also be given as to whether or not the surveillance activities of the Service take place where similar activities are also being undertaken by another agency e.g. the Police, Benefits Agency, Environment Agency.

Set a date for review of the authorisation and review on only that date.

Allocate a unique Reference Number (URN) for the application as follows:

Year Department Number of Application

Ensure that any RIPA Departmental Register is duly completed and that a copy of the RIPA forms (and any review/cancellations/renewal of the same is forwarded to Head of Legal and Democratic Services (Central Register) within 1 week of the relevant authorisation, review, cancellation and renewal.

9.5 **Who Can Grant Authorisation?**

The Regulation of Investigatory Powers ((Directed Surveillance and Covert Human Intelligence Sources) Order *2010*, prescribes that in a local authority, authorisations for Directed Surveillance and the use of a CHIS should be granted to Director, Head of Service, or equivalent. There is no provision for officers of a lower rank to grant authorisations even in cases of urgency. Authorisation for Direct Covert Surveillance or the use of CHIS must be given in writing by the Authorising Officer accept in urgent cases, when an authorisation may be given verbally. **Appendix 1** sets out the rank of officers empowered to grant authorisations.

9.6 In order to ensure greater independence and consistency, the power to grant, extend and discontinue authorisations will be limited to these officers only. The list will be maintained by the Head of Legal and Democratic Services. **Appendix 5** details the special arrangements for authorising surveillance where confidential material may be involved.

9.7 Authorising Officers should receive training in Human Rights and the Regulation of Investigatory Powers Act Legislation at the earliest possible opportunity and trained officers should be used in preference to those not having received training.

If a chief officer wishes to add, delete or substitute a post he/she must refer such a request to Head of Legal and Democratic Services.

9.8 **The Process of Obtaining an Authorisation**

Officers are advised to discuss the need to undertake Direct Covert Surveillance or the use of

a CHIS with their line manager before seeking authorisation. All other options to gain the information required should be fully explored before consideration is given to the use of covert techniques.

9.9 All requests to **conduct, review, review or cancel** a covert surveillance exercise or use a CHIS must be made in writing on the appropriate forms, as specified by the Office of Surveillance Commissioners (see **Appendix 3** and **4)** and be submitted to an appropriate Authorising Officer of the Council in a different Division to the Officer making the request(**Appendix 1**). Sufficient time should be given for the Authorising Officer to consider the application and for the Requesting Officer to obtain a formal order from a Magistrate.

9.10 All Requests must be considered and authorised in writing by an Authorising Officer **and an order from a Magistrate obtained by the Requesting Officer before any Directed Surveillance or CHIS operation can commence.** (See Appendices 6, 7 and 8).

9.11 Both the Requesting Officer seeking the authorisation and the Authorising Officer shall have regard to the factors detailed in paragraphs 9.3, 9.4 and 9.15 in respect of granting authorisations.

9.12 **Backdated Authorisation**

In ***no*** circumstance must any covert surveillance operation or CHIS be given backdated authorisation after it has commenced. Embarking upon Directed Surveillance or the use of a CHIS without authorisation or conducting covert surveillance outside the scope of the authorisation will not only mean that the 'protective umbrella ' of RIPA is unavailable but may result in disciplinary action being taken against the officer/officers concerned within the Council Personnel Policies and Procedures.

9.13 **Information to be provided in Applications for Authorisation**

A written application for authorisation for Direct Surveillance should describe any conduct to be authorised and the purpose of the investigation or nature of any surveillance.

The application should include:

- The grounds on which the authorisation is sought.
- The criminal offence you are investigating and how it satisfies the six month threshold test (see paragraph 9.4).
- The reasons why the authorisation is **necessary** in the particular case and the ground i.e. See paragraph; 9.4 *for the purpose of preventing or detecting crime.*
- The reasons why the surveillance is considered **proportionate** to what it seeks to achieve. *In particular the following elements of proportionality should 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 target and other*s
    - *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*
- The action to be authorised;
- The nature of the surveillance;
- An account of the investigation or operation;
- The identities, where know, of those to be the subject of the surveillance; an explanation of the information which it is desired to obtain as a result of the surveillance;
-
- The details of any potential collateral intrusion and why the intrusion is justified;
- The details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- The level of authority required (or recommended where that is different) for the surveillance; and
- A subsequent record of whether authority was given or refused, by whom and the time and date.

9.14 **<u>Records of Authorisations</u>**

A record of all authorisations must be maintained for five years. This should include not only those authorisations granted, but also those which are refused.

9.15 These records will be maintained by a nominated Authorising Officer, within each service. A copy must also be supplied to the **central record** of authorisations maintained by the Head of Legal and Democratic Services of Crawley Borough Council. **The Central Register will**

be maintained electronically as well as a hard copy.

9.16 Due to the sensitive nature of **all documentation** covered by the Act, consideration **MUST** be given to the means by which copies are forwarded either by hand or electronically.

9.17 **Grounds for Granting Authorisations**

Surveillance must be shown to be necessary. (Investigations can only fall into the following category):

- For the purpose of preventing or detecting crime **(see Section 22(2)(b), 28(3)(b) and 29(3)(b) RIPA** and
- The crime under investigation is or would be punishable (whether on summary conviction or on indictment) by a maximum term of **at least 6 months imprisonment (see paragraph 9.4).**

9.18 **Duration of Authorisations**

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 as follows:

- Directed Covert Surveillance – 3 months (from authorisation)
- Covert Human Intelligence Source (CHIS) – 12 months (from authorisation)

NB: Whether the surveillance is carried out/conducted or not in the relevant period does not mean that the "authorisation" is spent, in other words the forms do not expire they have to be reviewed and or cancelled once they are no longer required.

9.19 **Review of Authorisations**

Once granted, an authorisation should be reviewed regularly (at least monthly) by the officer managing the case to assess whether or not the investigation continues to be **necessary** and **proportionate**. The Authorising Officer should be notified of any instances where these criteria are no longer met.

9.20 The forms attached at **Appendix 3** and **4** should be used in conducting a review of Covert Surveillance or a CHIS. **(Form 3.3 and 4.3)**

9.21 The Results of a review should be recorded on the Central Register of Authorisations maintained by Legal and Democratic Services. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential material or involves collateral intrusion.

9.22 **Renewal of Authorisations**

If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given they may renew it in writing for a further period of 3 months.

9.23 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end and must be submitted to a Magistrate by the Requesting Officer for judicial approval before it can take effect. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

9.24 An application for renewal should be made to the officer who granted the original authorisation unless there is very good reason not to do so (e.g. because the original authorising officer is on annual leave / has left the Authority).

9.25 Applications for renewal should be made using the forms shown at **Appendix 3** (Directed Covert surveillance) and **Appendix 4** (Use of CHIS). **(Forms 3.2. and 4.2)**

All applications for the **renewal** of an authorisation for Directed Covert Surveillance should record:

- Whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- Any significant changes to the information in paragraph **6.25**;
- The reasons why it is necessary to continue with the directed surveillance;
- The content and value to the investigation or operation of the information so far obtained by the surveillance;
- The results of regular reviews of the investigation or operation.

9.26 Authorisations may be renewed more than once, if necessary, and the renewal should be kept /recorded as part of the central record of authorisations.

9.27 **Cancellation of Authorisations**

The Authorising Officer who granted or last renewed the authorisation **must** cancel it if they are satisfied that the investigation no longer meets the criteria upon which it was authorised. This should be undertaken following a recommendation from the officer managing the case, who will continually review the investigation against the criteria. Where the Authorising Officer is no longer available, this duty will fall on the person who is acting as Authorising Officer.

9.28 As soon as a decision is taken to cease the operation, an instruction must be given to those involved to stop all Directed Covert Surveillance / using the CHIS. A form recording the cancellation should be completed. The forms to be used are shown at **Appendix 3** and **4** (Directed Surveillance) and (Use of a CHIS) respectively. **(Forms 3.4 and 4.4)** The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation, where relevant.

10. Records Management

Crawley Borough Council must keep a detailed record of all Magistrate Approvals, Authorisations, Renewals, Cancellations and Rejections in Directorates/Departments and a Central Register of all Authorisations forms, Magistrates approvals, renewals cancellations and rejections will be maintained and monitored by the Head of Legal and Democratic Services.

10.1 **Recording Authorisations / Reviews / Renewals / Cancellations**

The originals of forms authorising/review/renewing/cancelling or rejecting Directed Surveillance or use of a CHIS should be forwarded within one week of the authorisation to the Head of Legal and Democratic Services. This information will be recorded on a Central Register. All forms should be retained for a period of not less than 3 years after the Surveillance has been discontinued. Similarly the relevant Directorate/Department shall

retain a copy of such forms for the same period.

10.2 **Records maintained in the Department**

The following documents must be retained by the relevant Director/Head of Service for such purposes.

- A copy of the forms together with any supplementary documentation and notification of the approval given by the Authorising Officer and a Magistrate;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the Authorised 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 Authorised Officer;
- The Unique Reference Number for the authorisation (URN)

Central Register Maintained by the *Head of Legal and Democratic Services*

Authorised Officers must forward details of each Form to the Head of Legal and Democratic Services for the Central Register, within 1 week of the authorisation, review, renewal, cancellation or rejection. The Head of Legal and Democratic Services will monitor the same and give appropriate guidance, from time to time, or amend this Document as necessary.

Crawley Borough 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.

Information required to be recorded on the Central Register:

- The type of authorisation;
- The date the authorisation was given;
- The date of the Order from the Magistrate;
- Name and position of the Authorising Officer;
- The unique reference number (URN) of the investigation; or operation
- The title of the investigation or operation, including a brief description and names of subjects, if known
- If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and name /position of the Authorising Officer and the date of the Order from the Magistrate;
- Whether the investigation or operation is likely to result in obtaining confidential information;
- The results of the review of the authorisation;

- The date the authorisation was cancelled
- A copy of the application and copy of the authority together with any supplementary documentation and notification of the approval given by the authorising officer.
- The record of the period over which the Surveillance has taken place.
- The reasons for any request being denied.

10.3 The Central Register will be maintained electronically as well as a hard copy.

10.4 The Head of Legal and Democratic Services will be responsible for monitoring authorisations, carrying out an annual review of applications, authorisations, refusals, extensions and cancellations and maintaining a centrally retrievable record of authorisations. Relevant Directorates must ensure that any data is processed in accordance with Data Protection legislation and in the case of use of CHIS's, records should be maintained in such a way as to preserve the confidentiality of the source and the information provided by the source.

11. Handling Product From Surveillance Activities

11.1 Product from Covert Surveillance activities may consist of:

- Photographs
- Video film
- Voice recordings
- Surveillance log
- Officers' Notes

11.2 The above may be required as evidence in current or future criminal proceedings. Officers must have regard to the provisions of the Criminal Procedure and Investigations Act 1996 in relation to unused material. Product obtained via an authorisation may be used by the authority in other investigations.

11.3 Although specific legislation and the Data Protection Act 1998 provide for the disclosure of information in certain circumstances, additional controls are introduced by the Regulation of Investigatory Powers Act.

11.4 The use of any product obtained by authorised surveillance activities outside of the Public Authority or the Courts should only be authorised in the most exceptional circumstances. This requirement seeks to prevent product from being used for grounds other than that for which it was obtained.

11.5 Officers may receive requests from other agencies for product which may include photographs of suspects, descriptions, vehicle details. Where this information has been obtained under an authorisation, further guidance should be sough from the Authorising Officer, since disclosure may not be permitted under the provisions of the Code of Practice

11.6 **Storage of Product**

11.7 Officers should ensure that evidential protocols are observed to ensure the integrity, security and confidentiality of material. The will ensure that the requirements of the Seventh Principle of the Data Protection Act are addressed. This principle deals with the security of data.

11.8 **Disposal of Product**

11.9 Officers should have regard to fifth principle of the Data Protection Act 1998, as follows: Product which is not required as evidence should not be retained any longer than necessary.

It will be necessary to retain product for a sufficient period of time to safeguard Crawley Borough Council against any civil claims against infringement of an individuals Human Rights. **A PERIOD OF FIVE YEARS** ensures that all of the retention period requirements are addressed.

11.10 Product which has been destroyed should have this fact recorded on the record of product obtained by Directed Surveillance, and be signed by the officer.

11.11 An amended copy of this Record form should be forwarded to the Authorising Officer, indicating destruction of the product obtained from the surveillance activity.

11.12 Relevant directorates must ensure that any data is processed in accordance with Data Protection Legislation.

11.13 In the case of use of CHIS's, records should be maintained in such a way as to preserve the confidentiality of the source and the information provided by the source.

12. Use of Covert Surveillance Equipment

12.1 Each department shall keep a record of equipment held and to be used for the purposes of RIPA. A copy of the list of equipment should be forwarded to the Head of Legal Services in order for the central record of all equipment held by the Council to maintained and be kept up to date.

12.2 The equipment is to be held by the individual departments should be accessible by other departments within the Council in order to carry out the functions under RIPA. Appropriate training must be given to the individual installing and using the equipment to ensure that the equipment is correctly installed and that data recorded is fit for purpose and meets the objectives of the investigation.

12.3 The impact on necessity and/or proportionality will be directed related to the type of equipment used. Any equipment used must be fit for purpose in meeting the objectives of the investigation. It is therefore important for the authorising officer to be informed of what equipment is being used and its capabilities [i.e. range, how its turned on manually or remotely] on the application form so that due consideration can be given when considering whether or not to grant the authorisation. The authorising officer will also need to give consideration and advise how images will be managed, for example images will not be disclosed without first speaking with the data controller to ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by the Council.

12.4 When equipment has been installed a check should be undertaken at least every 48 hours if not daily in order to ensure it remains operational.

12.5 Covert Surveillance Equipment will only be installed with the necessary authorisation of the Council's authorising Officers. It will only be installed in residential premises if a member of the public has requested help or referred a complaint to the Council and such matter can only be investigated with the aid of covert surveillance techniques after all the issues referred to in paragraphs 9.3, 9.4 and 9.15 have been considered. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant.

12.6 Any request by a Council Officer to a resident to keep a video/audio/written diary as part of a Covert evidence-gathering exercise will be regarded as a covert surveillance exercise conducted on behalf of the council and must be authorised.

12.7 Recording sound (with a DAT Recorder) on private premises could constitute Intrusive Surveillance unless it is done overtly e.g. it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues.

13. CCTV

13.1 Surveillance can also be by way of hidden cameras in public place or by targeted CCTV. That is where a CCTV camera is trained on a specific person or a spot at a particular time in order to observe the activities of a particular person or group of persons. That being said, where CCTV is used in the monitoring of public areas in an overt way and just happens to catch a criminal act, then this would not be classified as covert surveillance. However, there may be occasions where a covert CCTV System is used for the purposes of a specific investigation or operation, in which case, an application for Directed Covert surveillance will be required.

13.2 Reference should be made to the Council's Code of Practice on CCTV.

14. Internal Review of the use of RIPA

14.1 Within every local authority it is considered good practice for a senior responsible officer to be made responsible for:

- the integrity of the process in place within the local authority for the management of CHIS/Directed Surveillance
- compliance with Part II of the Act and with the Codes of Practice
- oversight of the reporting of errors to the relevant Commissioner and the identification of both the cause(s) or errors and the implementation of processes to minimise repetition of errors
- engagement with the Officer of the Surveillance Commissioner inspectors when it conducts its inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

14.2 Within local authorities, the senior responsible officer will be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioner. Where an inspection report highlights concerns about the standards of authorising officers, senior responsible officer will be responsible for ensuring the concerns are addressed. The responsible officer for the Council is the Head of Legal and Democratic Services.

15. Social Networking Sites and Internet Sites

15.1 Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether RIPA authorisation should be obtained.

15.2 Care must be taken to understand how the social media site being used works. Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

15.3 Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking site,

and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

15.4 CHIS authorisation is only required when using an internet trading organisation such as E-Bay or Amazon Marketplace in circumstances when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at this stage.

Further guidance on this activity is contained in the OSC Procedures and Guidance Paragraph 289 (reproduced below.)

Covert surveillance of Social Networking Sites (SNS)

289. The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

289.1 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done)

16. Complaints / Information

16.1 Copies of the Codes of Practice on:

- Covert Surveillance
- Covert Human Intelligence sources

are available for reference by the public in reception at The Town Hall, The Boulevard, Crawley, West Sussex, RH10 1UZ

16.2 Information on the Investigatory Powers Tribunal and complaint forms relating to activities covered by RIPA are available to the public in reception at The Town Hall, The Boulevard, Crawley, West Sussex, RH10 1UZ

.

Appendices

Appendix 1	Councils Authorising Officers
Appendix 2	RIPA Flow Chart
Appendix 3	RIPA Forms: Directed Surveillance
Appendix 4	RIPA Forms: Covert Human Intelligence Source (CHIS)
Appendix 5	Special Arrangements for Authorising Surveillance where Confidential Material may be involved
Appendix 6	Seeking Magistrate Approval for RIPA Authorisation.
Appendix 7	Magistrates' Approval Process Flow Chart
Appendix 8	Magistrates' Authorisation Form

Appendix 1 Covert Surveillance

Council's Authorising Officers

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order *2010*, prescribes that in a local authority, authorisations for Directed Covert Surveillance and the use of a CHIS should be granted to *Directors, Head of Service, and more senior posts* or equivalent. Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved although it is recognised that this may sometimes be unavoidable. Where an authorising officer authorises such an investigation or operation the central record of authorisation should identify this.

The power to grant, renew, review, cancel and reject authorisations will be limited to only those officers detailed below in order to ensure greater independence and consistency. The Head of Legal and Democratic Services will maintain this list. If a Chief Officer wishes to add, delete or substitute a post he/she must inform Head of Legal and Democratic Services. Where knowledge of confidential material is likely to be acquired, reference should be made to the special arrangements set out in **Appendix 5**.

Authorising Officers should receive training in Human Rights and the Regulation of Investigatory Powers Act Legislation at the earliest possible opportunity and trained officers should be used in preference to those not having received training.

Peter Browning - Deputy Chief Executive

Karen Dodds - Head of Crawley Homes

Karen Hayes - Head of Finance Revenues and Benefits

Lucasta Grayson - Head of People and Technology

Nigel Sheehan - Head of Partnership Services

No officer with direct involvement in an operation should authorise the use of RIPA unless it is unavoidable. If considered to be unavoidable the centrally record should record that an officer with direct involvement in the operation has authorised the use of RIPA.

Appendix 2

RIPA FLOW CHART

Requesting Officer ('The Applicant') must:

- Read the Corporate Policy & Procedures Document and be aware of any other guidance issued by the Head of Legal and Democratic Services.
- Determine that directed surveillance and/or a CHIS is required.
- Assess whether authorisation will be **in accordance with the law.**
- Assess whether the authorisation meets the directed surveillance **crime threshold**.
- 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 Authorised Officer.

Authorised Officer must:

- Consider in detail whether all options have been duly considered, including the Corporate Policy and Procedures Document and any other guidance issued by the Head of Legal and Democratic Services.
- 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.
- Ensure that the Requesting Officer obtains formal approval from the Magistrates Court **before** any surveillance is commenced.

The Applicant must:
REVIEW REGULARLY
(complete Review form) and submit to Authorised Officer on date set

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 Departmental Co-ordinator and to the Head of Legal and Democratic Services Services

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 need the same.

NB: If in doubt, ask the Head of Legal and Democratic Services BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected. Directors will designate one of their staff to be a Department Co-ordinator for the purpose of RIPA and advise the Head of legal and Democratic Services accordingly.

Appendix 3

RIPA FORMS: DIRECTED SURVEILLANCE

Appendix 3.1 Directed Surveillance Authorisation

Appendix 3.2 Review of Directed Surveillance Authorisation

Appendix 3.3 Renewal of a Directed Surveillance Authorisation

Appendix 3.4 Cancellation http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan?view=Binary

NB: If any doubt ask the Head of Legal and Democratic Services before any directed surveillance and for CHIS is authorised, renewed, cancelled or rejected.

Appendix 4

RIPA FORMS: Covert Human Intelligence Source (CHIS)

Appendix 4.1 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application?view=Binary

Appendix 4.2 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review?view=Binary

Appendix 4.3 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal?view=Binary

Appendix 4.4 http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation?view=Binary

NB: If in doubt, ask the Head of Legal and Democratic Services BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

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

MANAGEMENT OF COVERT HUMAN INTELLIGENCE SOURCES

Tasking

1. Tasking is the assignment given to the CHIS by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain, provide access to or disclose information. Authorisation for the use or conduct of a CHIS will be appropriate prior to any tasking where such tasking involves the CHIS establishing or maintaining a personal or other relationship for a covert purpose.

2. Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If the nature of the task changes significantly, then a new authorisation may need to be sought.

3. It is difficult to predict exactly what might occur each time a meeting with a CHIS takes place, or the CHIS 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 at a review (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further action is carried out.

4. Similarly, where it is intended to task a CHIS in a significantly greater or different 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 the existing authorisation is sufficient or needs to be replaced. This should be done in advance of any tasking and the details of such referrals must be recorded. Efforts should be made to minimise the number of authorisations per CHIS to the minimum necessary in order to avoid generating excessive paperwork.

Handlers and controllers

5. Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each CHIS.

6. Oversight and management arrangements for undercover operatives, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of public authorities.

7. The person referred to in section 29(5)(a) of the 2000 Act (the "handler") will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

8. The handler of a CHIS will usually be of a rank or position below that of the authorising officer.

9. The person referred to in section 29(5)(b) of the 2000 Act (the "controller") will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

Joint Working

10. In cases where the authorisation is for the use or conduct of a CHIS whose activities benefit more than a single public authority, responsibilities for the management and oversight of that CHIS may be taken up by one authority or can be split between the authorities. The controller and handler of a CHIS need not be from the same public authority.

11. There are many cases where the activities of a CHIS may provide benefit to more than a single public authority. Such cases may include:

- The prevention or detection of criminal matters affecting a national or regional area, for example where the CHIS provides information relating to cross boundary or international drug trafficking;
- The prevention or detection of criminal matters affecting crime and disorder, requiring joint agency operational activity, for example where a CHIS provides information relating to environmental health issues and offences of criminal damage, in a joint police/local authority anti-social behaviour operation on a housing estate;
- Matters of national security, for example where the CHIS provides information relating to terrorist activity and associated criminal offences for the benefit of the police and the Security Service.

12. In such situations, however, the public authorities involved must lay out in writing their agreed oversight arrangements.

13. Management responsibility for CHIS, and relevant roles, may also be divided between difference police forces where the Chief Officers of the forces concerned have made a collaboration agreement under section 23 of the Police Act 1996 or section 12 of the Police (Scotland) Act 1967, and the collaboration agreement provides for this to happen.

Security and Welfare

14. Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Also consideration should be given to the management of any requirements to disclose information tending to reveal the existence or identity of a CHIS to, or in, court.

15. The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

16. Where 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.

Appendix 5

Covert Surveillance

Special Arrangements for Authorising Surveillance Where Confidential Material may be Involved

Confidential material is particularly sensitive and is subject to additional safeguards. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the Authorising Officer should be at Director level or above.

An assessment should be made of how likely it is that the confidential material will be acquired.

Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The following general principles should be applied:

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

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

- It should be disseminated only where an appropriate officer (having sought advice from the Head of Legal and Democratic Services) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person where possession of it might prejudice any criminal or civil proceedings related to the information;

- Confidential information should be destroyed as soon as it is no longer necessary to retain it for a specific purpose.

Appendix 6

Seeking Magistrate approval for RIPA Authorisation

Officers should follow the following procedure:-

1. Complete and provide the completed RIPA authorisation form (and all necessary documentation or background information) to the Authorising Officer to enable him/her to make an informed decision recorded in writing on the form.

2. On receipt of the signed authorisation contact Legal Services and provide them with a copy of the authorisation, and any other relevant information.

3. Legal Services will review the authorisation and ensure compliance with the law and advise the Officer that he can proceed with the obtaining of the Magistrates approval before contacting the Magistrate's clerk.

4. The Officer will contract the Magistrates Clerk to arrange a hearing and give the Officer's dates to avoid for the following 14 days.

5. The Officer will complete the "Application for Judicial Approval for authorisation to obtain or disclose communications data to use a CHIS or to conduct directed surveillance form" (see Appendix 8) and produce a bundle for the Magistrate containing all the information relied upon

6. The Officer will notify Legal Services when the hearing date has been confirmed.

7. The Officer will attend the Magistrate's Court and present the case for approval of authorisation. The Officer will be required to answer questions about the surveillance which the Magistrate may wish to raise.

8. Whilst the original authorisation form will be shown to the Magistrate it will be given to and retained by Legal Services for the Council's central records and a copy provided to the Court.

9. The Order section of the form at paragraph 5 above will be completed by the Magistrate and will stand as the official record of the Magistrate's decision.

<u>Emergency Situations</u>

10. Where an Officer considers an application for authorisation requires urgent Magistrates approval they should contact Legal Services providing all relevant information as at paragraph 3 above, with the addition of a brief outline of why the matter should be heard quickly.

11. Legal Services will liaise with the Court Clerk to affect a quick hearing where it has been assessed as necessary to do so. A delay in internal procedures does not constitute an acceptable reason for an urgent Magistrate's listing.

12. A Magistrate may consider an authorisation out of hours in **exceptional circumstances.**

Note: Legal Services can assist the Officer with the above process and attend the Magistrates Court with the Officer if required.

Hearing Outcome

13. On the outcome of an application the Magistrate may impose any of 3 determinations:

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

    2. Refuse to approve the grant or renewal of an authorisation notice.

    3. Approve the grant or renewal of an authorisation notice.

14. Should a Magistrate quash an authorisation this means that the application was found to be fundamentally flawed. The Council in such circumstances will be given 2 business days to make representations should it wish to do so as to why the authorisation should not be quashed should it wish to do so. If an authorisation is quashed it cannot rely on it and a fresh authorisation will be required before further approval is sought.

15. Should a Magistrate refuse to grant an approval the Council could consider reapplying following consideration of the reasons for that refusal.

16. In the case of any reapplication or submission, Legal Services will provide advice and draft the appropriate paperwork where appropriate.

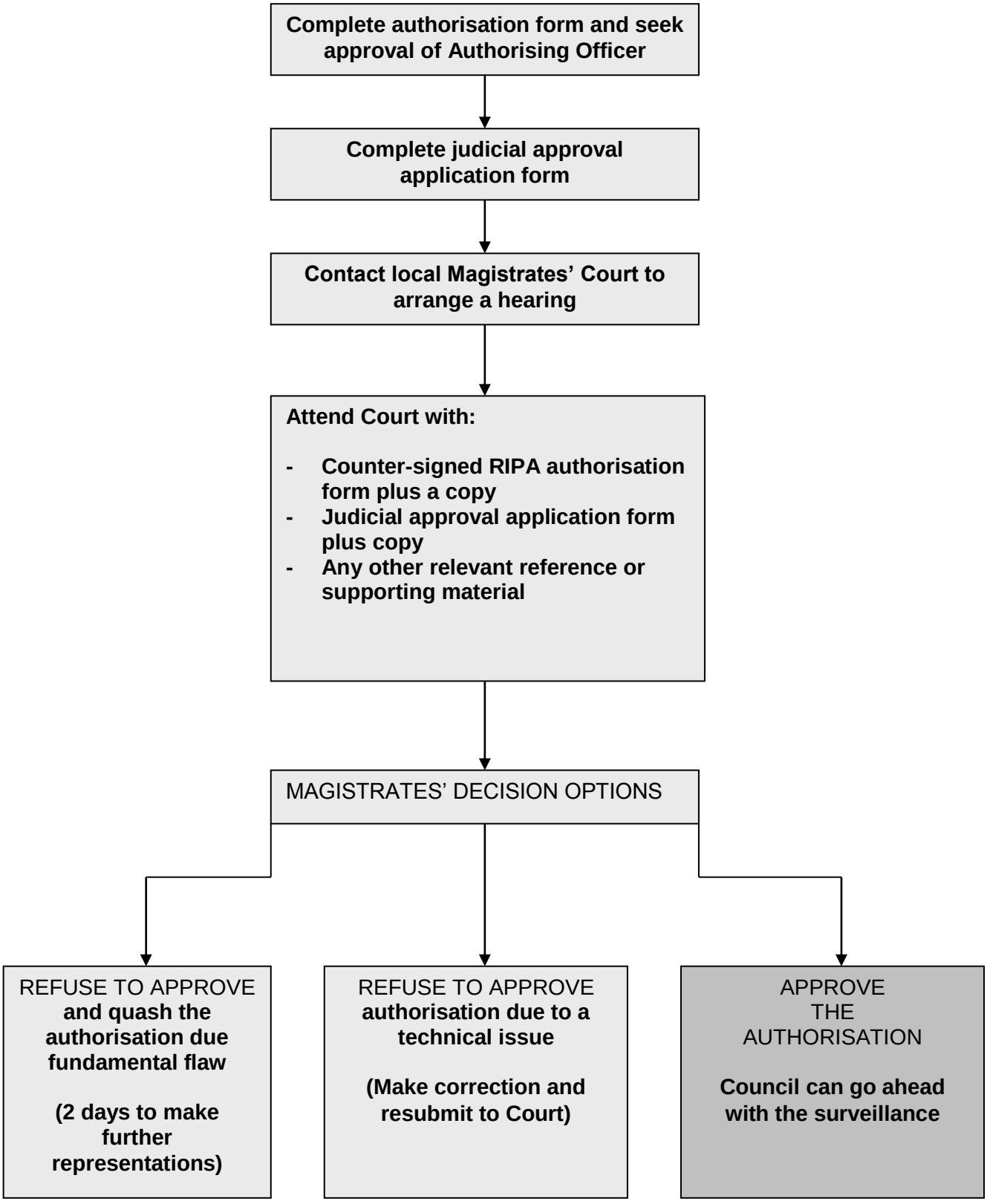
17. Where the Magistrate approves an authorisation notice the surveillance may lawfully take place for the period it is granted.

18. All renewals must be put before a Magistrate following referral to Legal Services and the same process as above followed. Cancellations and Reviews are not required to be placed before a Magistrate.

19. There is no right of appeal following a determination by a Magistrate except by way of Judicial Review on a point of law.

Appendix 7

The Magistrates' Approval Process



Appendix 8

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority: ……

Local authority department: ……

Offence under investigation: ……..

Address of premises or identity of subject: ……..

……

……

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

……..

……..

……..

……..

……..

……..

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer: ……

Authorising Officer/Designated Person: ……..

Officer(s) appearing before JP: ……..

Address of applicant department: ……..

……..

Contact telephone number: ……

Contact email address (optional): ……..

Local authority reference: ……

Number of pages: ……

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court: ……..

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

……..
……..
……..
……..
……..

Reasons

……..
……..
……..
……..
……..
……..

Signed:

Date:

Time:

Full Name:

Address of magistrates' court: