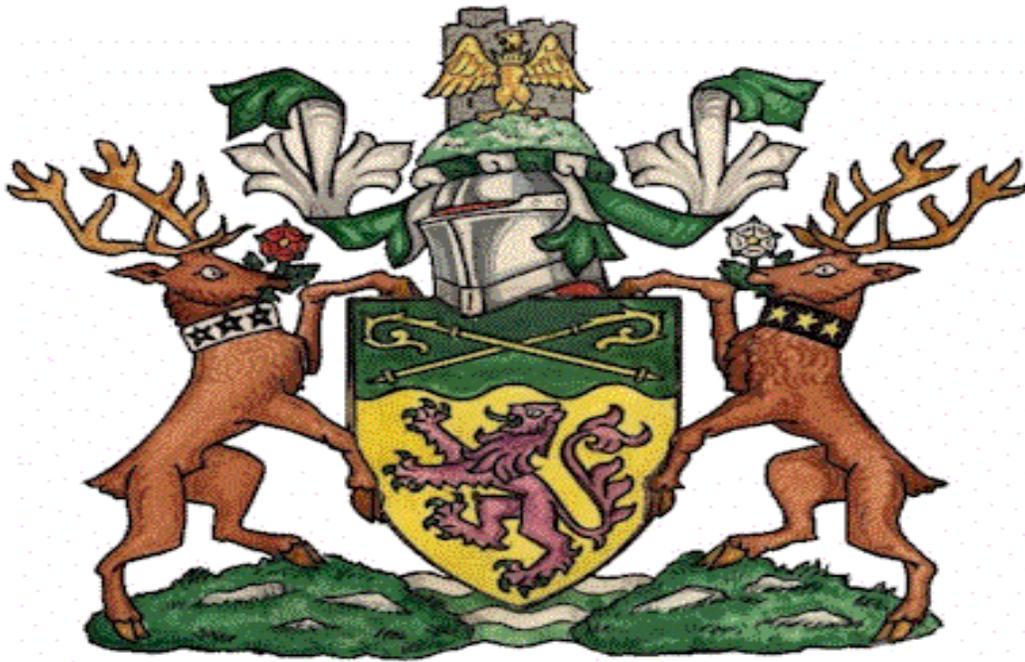


Ribble Valley Borough Council



Corporate Policy in Respect of Regulation of Investigatory Powers Act 2000 (“RIPA”)

November 2012

INDEX

Item	Description	Page
1.	Introduction	3
2.	Legislative Background	3-5
3.	Surveillance	6-8
4.	Covert Human Intelligence Sources	8-11
5.	Authorisation Process	11-18
6.	Authorising Officers	18-19
7.	Records and Central Register	18-20
8.	Complaints	20
9.	Appendices	
	• Appendix 1 - Code of Conduct on Directed Surveillance	21
	• Appendix 2 – Code of Conduct on Covert Human Intelligence Sources	21
	• Appendix 3 – Directed Surveillance Authorisation Flow Chart	22

1. INTRODUCTION

- 1.1 This Corporate Policy is based upon the requirements of the Regulation of Investigatory Powers Act 2000 (“**RIPA**”), and the Home Office’s Code of Practice for Covert Surveillance, and Covert Human Intelligence Sources (“**CHIS**”) (the “**Codes**”).
- 1.2 Ribble Valley Borough Council (the “**Council**”) has also taken into account and incorporated the guidance given by the Office of Surveillance Commissioners in its report dated 4 June 2008 and August 2011, and is grateful to it for providing this.
- 1.3 On 18 November 2008 the Head of Legal and Democratic Services was authorised by the Council’s Policy and Finance Committee to carry out periodic reviews of this policy and to amend it to the extent necessary to keep it up to date and in line with the Home Office’s Codes of Practice.
- 1.4 Whilst this policy provides guidance it is not intended to be an authoritative source on the provisions of RIPA. All Officers must therefore make reference to RIPA itself and to the Codes for an authoritative position.
- 1.5 Should any Officer be uncertain in respect of any aspect of RIPA, the authorising procedures set out in this policy, or at all, they should contact the legal department of the Council immediately.

2. LEGISLATIVE BACKGROUND

- 2.1 The Human Rights Act 1998 (the “**HRA**”) incorporated the European Convention on Human Rights (the “**ECHR**”) into domestic law.
- 2.2 Article 8 of the ECHR provides that:

“1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. *There shall be no interference by a public authority with the exercise of this right except such as is **in accordance with the law** and is **necessary** in a democratic society in the interests of national security, public safety or the*

economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protections of the rights and freedoms of others.” [Emphasis added]

2.3 There is therefore a qualified right for interference with individual’s rights under Article 8 if it is:

2.3.1 done in accordance with the law;

2.3.2 necessary; and/or

2.3.3 proportionate.

2.4 Any individual undertaking surveillance and/or using CHIS on behalf of the Council will therefore be breaching a person’s human rights unless that surveillance is authorised in accordance with the law, is necessary for one of the reasons set out above, and is proportionate.

2.5 This could have serious implications for the Council, not only in terms of its reputation, but could also potentially render any evidence gathered during the surveillance inadmissible in criminal proceedings, leave the Council open to civil proceedings for a breach of an individual’s human rights, and/or lead to a complaint being made to the Ombudsman. To avoid such a situation arising therefore, Officers must not carry out either Surveillance and/or CHIS unless the provisions of paragraph 2.3 are complied with.

In accordance with the law – RIPA

2.6 RIPA came into force on 25 September 2000, with the Codes subsequently coming into force pursuant to Section 71 of RIPA. The aim of RIPA was to strike a balance between protecting individuals’ rights under Article 8 ECHR and the HRA and the need for investigatory powers to protect the interests of society as a whole. It therefore allows interference with individuals’ rights in certain circumstances.

Necessity

- 2.7 It should be noted that pursuant to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Statutory Instrument No. 2010/521 a local authority, (and hence the Council) can only rely on Section 28 (3) (b) of RIPA as a ground for its interference being necessary. Therefore, under RIPA any interference can **only** be necessary if it is “*for the purpose of preventing or detecting crime or of preventing disorder.*”
- 2.8 Regulation 7A of the 2010 Act limits this further so that Authorising Officers may only authorise surveillance in respect of a criminal offence which is punishable by a maximum term of at least 6 months imprisonment or which constitutes an offence under section 146, 147 or 147A of the Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).
- 2.9 However, not all applications for the purpose set out above will be necessary. The Authorising Officer, **must** be satisfied that it is necessary in all the circumstances. A judgment will have to be made on a case-by-case basis. Generally any such interference will be not be necessary if there is an alternative **overt** method which could be used to obtain the information. Authorising Officers should therefore satisfy themselves that all other methods have either been exhausted or are not practicable. Authorising Officers should also take care to record in the authorisation their reasoning as to why the action is necessary.

Proportionate

- 2.10 Once it has been established that such interference is necessary it must then be considered whether it is **proportionate** to what is to be achieved. The Authorising Officer should consider the following elements of proportionality (as set out in paragraph 3.6 of the Code):
- 2.10.1 Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- 2.10.2 Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

2.10.3 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; and

2.10.4 Evidencing as far as reasonably practicable what other methods had been considered and why they were not implemented.

2.11 Authorising Officers should also take care to record within the authorisation form the reasons why they consider that the action is proportionate.

Judicial Approval

2.12 Following authorisation by an Authorising Officer judicial approval must be obtain prior to any surveillance being undertaken. Section 32A(2) of RIPA states that “*The authorisation is not to take effect until such time (if any) as the relevant judicial authority has made an order approving the grant of the authorisation.*”

2.13 Section 32A(3) o RIPA further provides that:

“(3) The relevant judicial authority may give approval under this section to the granting of an authorisation under section 28 if, and only if, the relevant judicial authority is satisfied that-

at the time of the grant-

there were reasonable grounds for believing that the requirements of section 28(2) were satisfied in relation to the authorisation, and

the relevant conditions were satisfied in relation to the authorisation, and

at the time when the relevant judicial authority is considering the matter, there remain reasonable grounds for believing that the requirements of section 28(2) are satisfied in relation to the authorisation.

(4)For the purposes of subsection (3) the relevant conditions are –

(a) in relation to a grant by an individual holding an office, rank or position in a local authority in England or Wales, that-

the individual was a designated person for the purposes of section 28,

the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 30(3), and

any other conditions that may be provided for by an order made by the Secretary of State were satisfied,.....”.

- 2.14 The procedure for making an application for judicial approval is contained in ***The Magistrates' Court (Regulation of Investigatory Powers) Rules 2012 (SI 2012/2563)***.

3. SURVEILLANCE

What is surveillance?

- 3.1 Surveillance includes:

3.1.1 Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications;

3.1.2 Recording anything mentioned above in the course of authorised surveillance; and/or

3.1.3 Surveillance, by or with, the assistance of appropriate surveillance device(s).

- 3.2 Surveillance can be either overt or covert.

Overt Surveillance

- 3.3 The vast majority of surveillance, which the Council carries out, will be overt and will involve Officers and employees noting events in the course of their normal daily duties. This will not fall within the scope of RIPA and will not require an authorisation. For example, a dog warden who notes an offence being committed as he/she carries out their daily routine will not require RIPA authorisation.

Covert Surveillance

- 3.4 Covert surveillance is defined in section 26(9)(a) of RIPA. It provides that *"surveillance is covert if, and only if, it is carried out in a manner that is calculated to*

ensure that persons who are subject to the surveillance are unaware that it is or may be taking place”.

RIPA Part II

3.5 RIPA Part II applies to the following conduct:

3.5.1 Directed Surveillance

3.5.2 Intrusive surveillance

3.5.3 Covert Human Intelligence Sources

Directed Surveillance (Section 26(2) RIPA)

3.6 **Section 26(2)** defines directed surveillance as surveillance, which is:

3.4.1 Covert but not intrusive;

3.4.2 Undertaken for the purpose of a specific operation;

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

3.4.5 Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of surveillance.

3.7 **Section 26(10)** defines “private information” in relation to a person as *“including any information relating to his private or family life”*.

Intrusive Surveillance (Section 26(3)-(6))

3.8 **Section 26(3)** defines surveillance as intrusive if and only if it is covert surveillance that:

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

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

3.9 Pursuant to **Section 26 (5)** surveillance which:

39.1 Is carried out by means of a surveillance device in relation to anything taking place on a residential premises or in any private vehicle, but

3.9.2 Is carried out without that device being present on the premises or in the vehicle.

is not intrusive **unless** the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

3.10 Please note that there is **NO** provision for a local authority to authorise intrusive surveillance.

4. **COVERT INTELLIGENCE SOURCES (“CHIS”)**

Who is a CHIS?

4.1 **Section 26(8)** of RIPA defines a CHIS as a person who:

(a) Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within (b) & (c) below;

- (b) He covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- (c) He covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

4.2 This is defined further within **Section 26(9)(b)&(c)** so that:

4.2.1 A **purpose** will only be covert if, and only if, it is carried out in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

4.2.2 A **relationship** is used **covertly**, and information obtained is **disclosed covertly**, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

4.3 Hence, there is no use of CHIS if a member of the public offers information to the Council that may be material to an investigation of an offence, but there would be if the Council then asked that person to obtain further information.

Authorising a CHIS

4.4 An authorisation **must** be obtained for CHIS in the same way as for directed surveillance. A detailed explanation of the authorisation process is contained in **Section 5** below. However, in addition, to the process for considering whether an authorisation is justified, a CHIS should not be authorised if it does not comply with the requirements of **Section 29(5)** of RIPA.

4.5 **Section 29(5)** requires that:

4.5.1 There will at all times be a person holding an office, rank, or position with the relevant investigating authority who will have **day to day responsibility for dealing with the source** on behalf of that authority, and **for the source's security and welfare**;

- 4.5.2 There will at all times be another person holding an office, rank or position with the relevant investigating authority who will have **general oversight** of the use made of the source;
- 4.5.3 There will at all times be another person holding an office, rank or position with the relevant investigating authority who will have responsibility for **maintaining a record** of the use made of the source;
- 4.5.4 The records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State (**see below**); and
- 4.5.5 The records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.
- 4.6 With regard to paragraph 4.5.4 above the regulations are set out in the Regulation of Investigatory Powers (Source Records) Regulations 2000. These regulations can be found at www.security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments, and **must** be referred to by Officers.

Vulnerable Individuals

- 4.7 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, illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

Vulnerable individuals should only be authorised to act as a source in the most exceptional circumstances, and the Chief Executive may only give such an authorisation.

Juvenile sources

- 4.8 There are also special safeguards with regard to the use or conduct of juvenile sources (under 18 years).
- 4.9 A source under 16 years of age **must not** be authorised to give information against his parents or any person who has parental responsibility for him.
- 4.10 There are also further requirements within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI No. 2793), and in other cases authorisations should not be granted unless these provisions are complied with. A copy of this can be also be found at www.security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments, and must be referred to by all Officers
- 4.11 The duration of such an authorisation is **one month** instead of 12 months.
- 4.12 Notwithstanding the above, the Council has not to date utilised these powers and considers that it is rare that they would be used in the future. As such **only the Chief Executive** may authorise any application for the use of CHIS and Officers should contact the legal department before making any application.

5. **AUTHORISATION PROCESS**

- 5.1 Directed surveillance and/or the use of CHIS shall be lawful for all purposes, if the conduct is properly and legitimately authorised and an Officer's conduct is in accordance with the authorisation.
- 5.2 Therefore all officers must obtain an authorisation from an Authorising Officer and Judicial approval before undertaking either directed surveillance and/or the use of CHIS, to ensure that it is lawful. A flowchart setting out the steps to be taken is attached at **Appendix 3**
- 5.3 Authorisations will only be given where:
- 5.3.1 The directed surveillance and/or the use of CHIS is necessary in the interests of preventing or detecting crime or disorder; and
- 5.3.2 It is proportionate to the objective which it is intended to achieve,

- 5.4 The Authorising Officer **must** satisfy himself of this before granting the authorisation.
- 5.5 In particular the Authorising Officer must consider whether the activity could be carried out in an overt or less intrusive manner. If it could then this should be the preferred method.

Collateral Intrusion

- 5.6 Before granting an authorisation an Authorising Officer **must** take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation.
- 5.7 Wherever practicable measures should also be taken, to avoid or minimise unnecessary intrusion into the lives of those people.
- 5.8 The applicant should also have included an assessment of the risk of collateral intrusion in the application form and the Authorising Officer should consider this in making their decision.

Confidential Information

- 5.9 RIPA does not provide any special protection for “confidential information”.
- 5.10 Notwithstanding this, special care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information may be involved.
- 5.11 Confidential information includes, matters subject to legal privilege, confidential personal information or confidential journalistic material.
- 5.12 For example special care should be taken with **surveillance** where it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter’s spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

- 5.13 In cases where through the use of surveillance and/or CHIS, confidential information may be obtained, **only** the Chief Executive, or in his absence, a Director, may give authorisation.

Application Forms

- 5.14 All applications and authorisations **must** be made/granted on the relevant Home Office forms. Electronic copies of these forms are available on the Home Office website at www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms. If an officer has difficulty obtaining the correct form they should contact the Legal Department.

Urgent applications

- 5.15 In urgent cases an Authorising Officer may give authorisation **orally**. However, as soon as practicable thereafter, the applicant should produce a statement recording in writing that the Authorising Officer had expressly authorised the action.
- 5.16 It would not normally be considered to be urgent unless in the opinion of the Authorising Officer, the time which it would take for a written authorisation to be granted, would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.

Content of Application

- 5.17 The applicant must ensure that each application contains a **unique reference number** (“URN”). This must be inserted into the box at the top right hand corner of the relevant form. This should include a reference to their department, the year, and the number of the application during that year. Authorising Officers should not authorise any application, which does not contain this.
- 5.18 Applicants must also ensure that they complete all boxes within the forms. If done properly this will ensure compliance with RIPA’s requirements. However, to ensure that there is full compliance the details of RIPA’s requirements are set out below.

Application for Directed Surveillance

5.19 A written application for directed surveillance should include:

- 5.19.1 A description of the conduct to be authorised and the purpose of the investigation or operation.
- 5.19.2 the reason(s) why the authorisation is necessary and the ground on which it is considered necessary pursuant to Section 28(3). As set above the only ground on which the Council can now rely is “*for the purpose of preventing or detecting crime or disorder*”.
- 5.19.3 the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- 5.19.4 the nature of the surveillance;
- 5.19.5 the identities, where known of those to be the subject of the surveillance;
- 5.19.6 an explanation of the information, which it is desired to obtain as a result of the surveillance;
- 5.19.7 the details of any collateral intrusion and why the intrusion is justified;
- 5.19.8 the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- 5.19.9 the level of authority required (or recommended where that is different) for the surveillance; and
- 5.19.10 a subsequent record of whether authorisation was given or refused, by whom, and the date and time.

Application for the use of CHIS

5.20 An application for the use or conduct of a source should include:

- 5.20.1 the reasons why the authorisation is necessary, and the grounds listed in section 29(3). Again, the only ground upon which the Council can rely is “*for the purpose of preventing or detecting crime or disorder*”;
- 5.20.2 the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- 5.20.3 the purpose for which the source will be tasked or deployed;
- 5.20.4 where a specific investigation or operation is involved, the nature of that investigation or operation;
- 5.20.5 the nature of what the source will be tasked to do;
- 5.20.6 the level of authority required (or recommended where different);
- 5.20.7 the details of any potential collateral intrusion and why the intrusion is justified;
- 5.20.8 the details of any confidential information that is likely to be obtained as a consequence of the authorisation; and
- 5.20.9 a subsequent record of whether authority was given or refused, by whom and the time and date.

Duration Of Authorisations

Directed Surveillance

- 5.21 A written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.
- 5.22 Urgent oral authorisations or written authorisations granted by a person who is only able to grant authorisations in urgent cases, will unless renewed cease to have effect

after **seventy two hours**, beginning with the time when the authorisation was granted or renewed.

CHIS

5.23 A written authorisation will unless renewed cease to have effect at the end of a period of **twelve months** beginning with the day on which it took effect.

5.24 Urgent oral authorisations or written authorisations granted by a person who is only able to grant authorisations in urgent cases, will unless renewed cease to have effect after **seventy two hours**, beginning with the time when the authorisation was granted or renewed.

Reviews

5.25 Regular reviews should be carried out to assess the need for the authorisation to continue. Reviews should take place frequently if the source of surveillance provides confidential information or involves collateral intrusion.

5.26 The Authorising Officer must decide how frequently and when the reviews should take place. This should be as frequently as is considered necessary and practicable.

5.27 The Authorising Officer must use the appropriate form to complete the review, and the results of the review should be recorded in the central record of authorisations.

Renewals

5.28 If at any time before an authorisation ceases to have effect an Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given he may renew it for:

5.28.1 3 months (Directed Surveillance)

5.28.2 72 hours (Urgent Directed Surveillance)

5.28.3 12 months CHIS

5.28.4 72 hours (Urgent CHIS)

There should however be no circumstances in which an authorisation is subject to an urgent renewal.

5.29 The renewal will take effect at the time at which, or the day on which the authorisation would have ceased to have effect but for the renewal.

5.30 An application for renewal of an authorisation should not be made until shortly before the authorisation is due to cease to have effect.

5.31 Any person who would be entitled to grant a new authorisation is able to renew an authorisation.

5.32 An authorisation can be renewed more than once as long as it continues to meet the criteria for authorisation.

5.33 The application for renewal must include:

Directed Surveillance

- Whether this is the first renewal of an authorisation on which the authorisation has been renewed previously;
- Any significant changes to the information included in the original application;
- 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; and
- The results of regular reviews of the investigation or operation.

CHIS

- Whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- Any significant changes to the information in the original application;
- The reasons why it is necessary to continue to use the source;
- The use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation;
- The tasks given to the source during that period and the information obtained from the conduct or use of the source; and
- The results of regular reviews of the use of the source.

5.34 **As with new applications judicial approval must also be sought after the Authorising Officer gives authorisation.**

Cancellations

- 5.35 The Authorising Officer who granted or last renewed the authorisation **must** cancel it if he is satisfied that it no longer meets the criteria under which it was first granted.
- 5.36 The Authorising Officer must complete the relevant form to do so and pass the information to the legal department to be included on the central register.
- 5.37 In addition, when the decision is taken to stop surveillance, an immediate instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central register and on the cancellation form.
- 5.38 There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation but effective practice suggests that a record

should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

6. AUTHORISING OFFICERS

6.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI 2010 No. 521 provides that the Director, Head of Service, Service Managers, or equivalent officer may give authorisations for directed surveillance and CHIS under RIPA.

6.2 In light of the infrequent use made of RIPA and CHIS and based on advice given by the OSC, Ribble Valley Borough Council has resolved that it will only have three Authorising Officers who will be the Chief Executive, the Director of Community Services, and the Director of Resources. These Officers will receive regular training to enable them to deal properly with all authorisations.

6.3 Moreover, applicants must submit their application to an Authorising Officer, from outside of their department.

7. RECORDS AND CENTRAL REGISTER

7.1 The Council's Legal Department will maintain a central record of all authorisations. This will be updated whenever an authorisation is granted, renewed, or cancelled.

7.2 The record will be retained for a period of at least **three years** from the end of the authorisation and will contain the following information:

7.2.1 the type of authorisation;

7.2.2 the date the authorisation was given;

7.2.3 Name and rank/grade of the authorising officer, the unique reference number (URN) of the investigation or operation;

- 7.2.4 the title of the investigation or operation, including a brief description and names of subjects, if known, whether the urgency provisions were used, and if so why;
 - 7.2.5 if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer;
 - 7.2.6 whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
 - 7.2.7 the date the authorisation was cancelled; and
 - 7.2.8 whether there has been a “self authorisation”.
- 7.3 In respect of each step in the procedure Authorising Officers **must** retain all original documentation **and must** give to the legal department a copy of the following information:
- 7.3.1 the application, authorisation and notice of judicial approval together with any supplementary documentation and notification of the approval given by the authorising officer;
 - 7.3.2 a record of the period over which the surveillance has taken place;
 - 7.3.3 the frequency of reviews prescribed by the authorising officer;
 - 7.3.4 a record of the result of each review of the authorisation;
 - 7.3.5 the renewal of an authorisation, and any judicial approval given together with the supporting documentation submitted when the renewal was requested; and
 - 7.3.6 the date and time when the Authorising Officer gave any instruction.
- 7.4 For the avoidance of doubt the information set out above must be passed to the legal department contemporaneously to ensure that the Council’s central record can be

maintained and that the Council can therefore ensure that all authorisations are reviewed and cancelled in accordance with RIPA.

8. COMPLAINTS

8.1 Any person who reasonably believes that they have been adversely affected by surveillance activity and/or the use of a CHIS, by or on behalf of the Council may complain to the Legal Services Manager (as Monitoring Officer) who will investigate the complaint.

8.2 They may also complain to:

The Investigatory Powers Tribunal
PO Box 33220
London SW1H 92Q

9. APPENDICES

1.	Code of Practice on Covert Surveillance - www.security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/
2.	Code of Practice on Covert Human Intelligence Sources - www.security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/
3.	Directed Surveillance Authorisation Flow Chart

APPENDIX 3 – DIRECTED SURVEILLANCE

Before making an application for directed surveillance, all applicants **must**:

- ❖ read the RVBC RIPA corporate policy and satisfy themselves that they understand its requirements before proceeding;
- ❖ decide whether the directed surveillance is in accordance with the law
- ❖ decide whether directed is necessary pursuant to S.28(3)(b) i.e.: “for the purpose of preventing or detected crime or disorder and relate to a criminal offence the maximum punishment for which is 6 months imprisonment;

It will not be necessary if a less intrusive method is available and practicable.

- ❖ decide whether directed surveillance is proportionate to the aims which it seeks to achieve;
- ❖ consider whether there will be collateral intrusion or whether confidential information will be obtained.

If in doubt please contact the legal department for advice!!

If the directed surveillance is necessary and proportional, complete the relevant form in full ensuring that it has a URN

Seek oral authorisation if the matter is urgent, and record in writing that oral authorisation was given by the authorising officer as soon as practicable thereafter

An Authority Officer who receives an application must:

- ❖ decide whether the directed surveillance would be in accordance with the law;
- ❖ decide whether the directed surveillance would be necessary pursuant to S.28(3)(b) ie: “for the purpose of preventing or detected crime or disorder” and relate to a criminal offence the maximum punishment for which is 6 months imprisonment;
- ❖ Consider whether all alternative less intrusive methods which are practicable been considered/exhausted.
- ❖ If appropriate, to authorise and complete the authorisation and set an appropriate review date.

Apply to the Magistrates Court for judicial approval.
ONLY PROCEED IF APPROVAL GRANTED

- ❖ A review must take place on the date set by the Authorising Officer.
- ❖ The applicant must submit a review form to the Authorising Officer in advance of this.

If at any time the directed surveillance is no longer necessary/proportionate for reasons for which it was granted the applicant should submit a cancellation form to the Authorising Officer and immediately inform those conducting the surveillance to stop. Details of the instruction should be recorded.

If the directed surveillance remains necessary and proportionate the applicant should apply for and the Authorising Officer should grant a renewal using the appropriate form before the authorisation ceases to have effect.

If the directed surveillance is no longer necessary or proportionate the Authorising Officer should cancel it.

Apply to Magistrates Court for judicial approval.
ONLY PROCEED IF APPROVAL GRANTED.

Authorising Officers should retain the originals of all forms/records and must forward a copy to the legal department so that they can be added to the central record.