REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY STATEMENT AND PROCEDURES

Version Control				
Document owner	Published	Version	Changed	Amended by
A Moppett	13/05/2015	V.1		
A Moppett		V.2		AJM

Contents

1. Introduction

Regulation of Investigatory Powers Act 2000 (as amended by the Protection of Freedoms Act 2012)

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) was enacted to provide a clear statutory framework for the operation of certain intrusive investigative techniques, to ensure compliance with the Human Rights Acts 1998. The main purpose of the Act is to ensure that individuals' rights are protected whilst allowing law enforcement and security agencies to do their jobs effectively and act proportionately.

1.2 RIPA covers the interception, acquisition and disclosure of communications data (Part I of RIPA); the carrying out of surveillance and use of covert human intelligence sources (Part II); and the investigation of electronic data protected by encryption (Part III).

1.3 Craven District Council is included within this framework with regard to Directed Surveillance and Covert Human Intelligence Sources (Sections 28 and 29 of the Act).

1.4 Craven District Council is **not** permitted to carry out Intrusive Surveillance involving entry on or interference with property or with wireless telegraphy as regulated by the Regulation of Investigatory Powers Act 2000.

1.5 This Policy will focus on the provisions of Part II of RIPA (as amended by the Protection of Freedoms Act 2012 (POFA) that cover the use and authorisation of directed surveillance and the steps that must be taken by Council Officers to comply with the Act.

1.6 Surveillance is used to target criminals but is also a means of protecting the public from harm and preventing crime.

1.7 The provisions of RIPA do not cover authorisation for the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime.

1.8 RIPA also provides for the appointment of independent Surveillance Commissioners who will oversee the exercise by public authorities of their powers and duties under the Act (Part IV of RIPA).

1.9 This Policy must be read in conjunction with the Home Office Code of Practice for Covert Surveillance and Property Interference and the Covert Human Intelligence Sources Code of Practice (2014 Editions).

2. Definitions

2.1 What is Surveillance?

Surveillance is:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications
- Recording anything monitored, observed or listened to in the course of surveillance
- Surveillance by or with the assistance of appropriate surveillance device(s).

Surveillance can be **overt** or **covert**.

2.2 Overt Surveillance

2.2.1 Most of the surveillance carried out by the Borough Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. For example, sign-posted CCTV cameras or a parking attendant patrolling a Council car park.

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

2.3 Covert Surveillance

2.3.1 Covert Surveillance as defined in Section 26 RIPA:

"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".

2.3.2 General observation forms part of the duties of many enforcement officers. It forms part of the everyday functions of law enforcement or other public bodies. This low level activity will not usually be regulated under the provisions of RIPA.

2.3.3 The installation of CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance which requires authorisation.

Members of the public are aware that such systems are in use, for their own protection and to prevent crime.

Authorisation may be required if a CCTV camera is being used for a specific type of surveillance.

2.4 Directed Surveillance (Section 26(2) RIPA)

2.4.1 Directed surveillance is surveillance which is covert and is conducted for the purpose of a specific investigation or operation in a manner likely to obtain. **private information**. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen.

2.4.2 Below are some examples where directed surveillance is conducted by the Council:

- Monitoring of noise complaints
- Monitoring of benefit claimants who have not declared that they are working/living with a partner etc.

2.5 Intrusive Surveillance (Section 26(3) RIPA)

2.5.1 **The Council cannot conduct intrusive surveillance** involving entry on or interference with property or with wireless telegraphy as regulated by the Regulation of Investigatory Powers Act 2000**.**

2.5.2 Surveillance is intrusive if it is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle where an individual present. This kind of surveillance may take place by means either of 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.

2.5.3 The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels constitutes neither directed nor intrusive surveillance.

2.6 Covert Human Intelligence Source (CHIS) (Section 26(8) RIPA)

A person is a covert human intelligence source (CHIS) if:

- he establishes or maintains a personal or other relationship with a person for the *covert purpose* of facilitating one or both of the following;
- he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

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

In establishing or maintaining a relationship, a *covert purpose* exists where the relationship is conducted in such a manner that it is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

2.7 Private Information

"Private information", in relation to a person, includes any information relating to his private or family life and aspects of business or professional life.

2.8 Private Vehicle

"Private Vehicle" means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use the vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey.

2.9 Confidential Material

This consists of:

- **Matters subject to legal privilege** - for example oral and written communications between a professional legal adviser and his client or any person representing his 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.

- **Confidential personal information** - which is information held in confidence concerning an individual (living or dead) who can be identified from it, and relating to a) his physical or mental health or b) to spiritual counselling or other assistance given or to be given, and which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office.

- **Confidential journalistic material** - which includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

- **Communications between a Member of Parliament and another person on constituency matters**.

2.10 Residential Premises

"Residential premises" means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

2.11 Right to Privacy

Great care is required as the right to privacy (Article 8 Human Rights Act 1998) can also extend to business premises or residential premises used for business purposes.

2.12 Collateral Intrusion

This is interference with the privacy of a person other than the surveillance subject.

2.12.1 Before authorising applications for directed surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance activity.

2.12.2 Measures should be taken, wherever practicable, to avoid or minimise the unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion in considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

2.13 Authorising Officer

This is a person within the Council designated, for the purpose of the Act, to grant authorisation for directed surveillance. The Council's Authorising Officers are listed in Appendix A.

2.14 RIPA Monitoring Officer

This is an internal role performed by the Solicitor to the Council. The role involves maintaining policies and procedures, providing training and keeping a central record of all applications and liaising with the Office of the Surveillance Commissioner.

2.15 Senior Responsible Officer

The Senior Responsible Officer is responsible for the integrity of the Council's procedures to authorise directed surveillance or the use of CHIS. He is also responsible for ensuring compliance with the Act and the Codes of Practice and engagement with the Commissioners and Inspectors when they conduct their inspections and where necessary overseeing the implementation of any post-inspection actions plans recommended or approved by a Commissioner. The Council's Senior Responsible Officer is the Chief Executive.

2.16 Office of Surveillance Commissioners

The Office of Surveillance Commissioners is responsible for reviewing our activities carried out under RIPA 2000. All authorities are subject to review and inspection. Inspection will cover policy and procedures as well as individual

investigations.

2.17 Codes of Practice

The Home Office has issued two RIPA Codes of Practice which provide guidance on provisions in Part II of RIPA 2000. The Covert Surveillance and Property Interference Code of Practice and the Covert Human Intelligence Sources Code of Practice are available at www.gov.uk/guidance/.

2.16 All applications/authorisations, reviews, renewals and cancellations must be on the current Home Office approved forms which are available from the RIPA Monitoring Officer or at www.gov.uk/guidance/

3. Councillor's Role

3.1 Members of the Council's Audit and Governance Committee will agree the RIPA Policy Statement on an annual basis and will receive twice yearly reports on the Council's use of RIPA to ensure that it is being used in accordance with the Policy.

4. Authorisation of Directed Surveillance

4.1 **Authorisation of Surveillance**

4.1.1 **Since 1st November 2012, when the Protection of Freedoms Act 2012 amended RIPA 2000, the framework governing how local authorities use RIPA has changed. Authorisation of the use of certain covert powers, including the use of directed surveillance, will only have effect once an order approving the authorisation has been granted by a Justice of the Peace. This new judicial approval mechanism is in addition to the existing authorisation process. The current processes of assessing necessity and proportionality, completing the RIPA authorisation/application forms and seeking approval from an Authorising Officer remain the same.**

4.1.2 **Therefore, there is a two-stage process. First, an authorisation must be obtained from an Authorising Officer. Secondly, approval of the authorisation must be obtained from a Justice of the Peace. This involves applying to a Magistrates Court. Further detail about the judicial approval process is set out in paragraphs 3.1.17 to 4.1.22.**

4.1.3 Authorising Officers will be appointed by the Chief Executive if he is satisfied that they have had appropriate training to undertake the role. The Solicitor to the Council will maintain a record of Authorising Officers.

4.1.4 Written authorisations **must** be completed whenever an investigation involves the use of Directed Surveillance. This provides lawful authority to carry out covert surveillance. Authorisation **must** be sought before surveillance is undertaken.

4.1.5 All applications for authorisation of **Directed Surveillance** must be made on the appropriate Home Office approved application form (available on the Council's Intranet). The Investigating Officer will discuss with his/her Line Manager the action(s) to be authorised and decide, on a case by case basis, whether a risk assessment is required. A template surveillance risk assessment is available on the intranet. The Investigating Officer should obtain a unique reference number (URN) from the Solicitor to the Council. The application must include:

- the grounds on which authorisation is sought - the power to authorise surveillance exists only for the prevention and detection of crime and disorder and no other purpose

- Since November 2012, an authorisation for directed surveillance can only be granted where the Council is investigating specific categories of criminal offences. These categories are: criminal offences punishable by a maximum term of at least six months imprisonment or criminal offences relating to the underage sale of alcohol or tobacco contrary to Sections 146, 147 and 147A of the Licensing Act 2003 and Section 7 of the Children and Young Persons Act 1933.

- consideration of why the Directed Surveillance is proportionate to what it seeks to achieve;

- that other options for the gathering of information have been considered and that Directed Surveillance is necessary

- the identity or identities, where known, of those to be the subject of Directed Surveillance;

- the action to be authorised and level of authority required;

- an account of the investigation or operation;

- an explanation of the information which it is desired to obtain as a result of the authorisation;

- any potential for collateral intrusion;

- the likelihood of acquiring any confidential material.

4.1.6 The Directed Surveillance Crime Threshold was introduced by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 which came into force on 1st November 2012. The introduction of this new threshold means that the Council may continue to authorise the use of Directed Surveillance in more serious cases provided the other tests are met (i.e. that it is necessary and proportionate and that prior approval from a Justice of the Peace has been obtained). However, it also means that the Council may not authorise the use of Directed Surveillance to investigate disorder that does not involve criminal offences, or to investigate low level offences, which may include, for example, littering, dog control and fly-posting.

4.1.7 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. The original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

4.1.8 The Authorising Officer should first satisfy him/herself that the authorisation is **necessary** on particular grounds and that the surveillance is **proportionate** to what it seeks to achieve. It is important that sufficient weight is attached to considering whether the surveillance required is proportionate. These concepts of "necessity" and "proportionality" occur regularly throughout human rights law and RIPA and they must be considered afresh in the case of each authorisation of surveillance. Therefore this will involve balancing the intrusiveness of the surveillance on the target and others who might be affected by it against the need for the surveillance in operational terms. The surveillance will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All surveillance should be carefully managed to meet the objective in question and

must not be arbitrary or unfair.

4.1.9 When proportionality is being assessed, the following elements 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 adopted will cause the least possible intrusion on the subject and others
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of
- obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

4.1.10 The Authorising Officer must be able to produce evidence that the relevant issues have been considered for monitoring purposes, for example a note of the documents and information available to the officer at the time the authorisation is given, together with a note of the date and time authorisation was given. It is essential that the Authorising Officer considers each request for an authorisation on its merits and a rubber stamping approach must never be used.

4.1.11 The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a higher degree of privacy, for instance in his/her home, or where there are special sensitivities, such as where the surveillance may give access to confidential material or communications between a minister of any religion or faith and another individual relating to that individual relating to that individual's spiritual welfare.

4.1.12 Particular consideration should be given to collateral intrusion on, or interference with, the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used for any form of medical or professional counselling or therapy.

4.1.13 An authorisation request should include assessment of any collateral intrusion or interference. This will be taken into account, by the Authorising Officer, particularly when considering the proportionality of the surveillance.

4.1.14 Directed surveillance undertaken by the Council requires the written approval of a post holder identified in 4.1.16 of this document.

4.1.15 Authorising Officers should not be responsible for authorising their own activities, i.e. those directly involved in undertaking surveillance.

4.1.16 The following table identifies appropriate authorisation levels in the Council's staffing structure.

Type of Request	Authorising Officer
Written authorisation to conduct investigations using Directed Surveillance:	Officers specifically designated by the Chief Executive as Authorising Officers and named in the attached Appendix
Written authorisation to conduct investigations using Directed Surveillance likely to obtain confidential information:	Head of Paid Service (Chief Executive) or in his absence, the acting Head of Paid Service

4.1.17 **Judicial approval**

a) Where an Authorising Officer has granted an authorisation, for Directed Surveillance, the authorisation is not to take effect until a Justice of the Peace has made an order approving the grant of the authorisation.

b) A Justice of the Peace will only give approval to the granting of an authorisation for **Directed Surveillance** if they are satisfied that:

- at the time the Authorising Officer granted the authorisation, there were reasonable grounds for believing that the authorisation was necessary and that the surveillance being authorised was proportionate, that the Authorising Officer was a designated person for the purposes of section 28 of RIPA, that the grant of the authorisation was not in breach of any restrictions imposed by virtue of section 30(3) of RIPA, that any other conditions provided for by any Order were satisfied; and
- that there remain reasonable grounds for believing that the necessary and proportionate tests are satisfied.

c) If a Magistrates' Court refuses to approve the grant of the authorisation, then it may make an order to quash that authorisation.

4.1.18 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates Court of that authorisation has been obtained.

4.1.19 Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. The Council is required to make an application without notice to the Magistrates Court to seek judicial approval.

4.1.20 **Therefore, any Authorising Officer who proposes to approve an application for the use of directed surveillance must immediately inform the Solicitor to the Council who will then make arrangements for an application to be**

made by appropriate officer to the Magistrates Court for an order to approve the authorisation to be made.

4.1.21 There is no need for a Justice of the Peace to consider either cancellations or internal reviews.

4.1.22 The Council will provide the Justice of the Peace with a copy of the original RIPA authorisation form and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon. In addition, the Council will need provide the Justice of the Peace with a partially completed judicial application/order form. A draft application for judicial approval and draft order are available on the Council's intranet.

4.2 Duration of authorisations

4.2.1 A written authorisation for directed surveillance will cease to have effect at the end of a period of three months beginning with the day on which it took effect, which is the date on which Magistrates' approval is obtained.

4.2.2 All authorisations continue to exist even if no longer effective until cancelled. All authorisations must be cancelled when no longer required.

4.3 Renewals

4.3.1 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, he/she may approve a renewal in writing for a further period of three months, beginning with the day when the authorisation would have expired but for the renewal.

4.3.2 Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

4.3.3 All requests for the renewal of an authorisation for Directed Surveillance must be made on the Home Office approved renewal form (available on the intranet) and must record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- the information required in the original request for an authorisation, as listed in section 3.1.5 above together with;

(a) any significant changes to the information in the previous authorisation;

(b) why it is necessary to continue with the surveillance;

(c) the content and value to the investigation or operation of the information so far obtained by the surveillance;

(d) an estimate of the length of time the surveillance will continue to be necessary; and

(e) why it remains proportionate to renew or continue.

4.3.4 Renewals of authorisations will also be subject to approval by the Magistrates Court. The Authorising Officer must therefore advise the Solicitor to the Council immediately when they are minded to grant a renewal.

4.3.5 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but officers must take account of factors which may delay the renewal process (eg. intervening weekends or the availability of the Authorising Officer and a Justice of the Peace to consider the application).

4.4 Cancellations

4.4.1 The Authorising Officer must cancel an authorisation if he/she is satisfied that the Directed Surveillance no longer meets the criteria for authorisation. When cancelling an authorisation, an Authorising Officer must ensure that proper arrangements have been made for the activity's discontinuance, including the removal of technical equipment, and directions for the management of the product.

4.4.2 The Home Office approved cancellation form must be completed (available on the intranet) and a copy sent to the Solicitor to the Council.

4.5 Reviews

4.5.1 Authorising Officers will review all "Directed Surveillance" applications and authorisations that they have granted regularly. The results of a review should be recorded on the Home Office approved review form (available on the intranet), and kept in the central record of authorisations. The Authorising Officer should determine how often the review should take place. This should be done as frequently as is considered necessary and practicable, but not later than once a month following the date of authorisation; sooner where the surveillance provides access to confidential material or involves collateral intrusion.

4.5.2 Reviews of an authorisation for Directed Surveillance must record:

- Any significant changes to the information in the previous authorisation;
- why it is necessary to continue with the surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- an estimate of the length of time the surveillance will continue to be necessary; and

- why the authorisation remains proportionate.

4.6 Records and Documentation

4.6.1 All documentation regarding Directed Surveillance should be treated as confidential and should be kept accordingly.

4.6.2 Records should be maintained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable period, commensurate to any subsequent review.

4.6.3 If there is any reason to believe that the results obtained during the course of investigation might be relevant to that investigation or to another investigation or to pending or future civil or criminal proceedings then it should not be destroyed but retained in accordance with established disclosure requirements. Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996, which requires that material should be retained if it forms part of the unused prosecution material gained in the course of an investigation, or which may be relevant to an organisation.

4.6.4 Authorising Officers are reminded of the importance of safeguarding confidential and sensitive information. They must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

4.6.5 Each Service undertaking Directed Surveillance must ensure that adequate arrangements are in place for the secure handling, storage and destruction of material obtained through the use of covert surveillance.

4.6.6 The original of all authorisations and other RIPA documents must be sent to the Solicitor to the Council, so that there is a central record maintained, and so that in her role as the RIPA Monitoring Officer she can ensure the Act is being complied with.

4.7 Monitoring of Authorisations

4.7.1 Information must be supplied to the Monitoring Officer using the forms attached to this guidance. The Monitoring Officer will maintain a Central Register of all forms completed by the Authorising Officer. Authorising Officers are responsible for sending **the original authorisation** in the appropriate form for each authorisation, cancellation and renewal granted, to the Monitoring Officer for inclusion in the Central Register and keeping a **copy** for their own records in the individual departments.

4.7.2 A review will be carried out regularly to ensure all forms have been sent for inclusion in this Central Register. The Monitoring Officer is required by law to ensure that the Council does not act unlawfully.

4.7.3 Authorising Officers are required to ensure that:

- Authorisations have been properly cancelled at the end of the period of surveillance
- Surveillance does not continue beyond the authorised period
- Current authorisations are regularly reviewed
- At the anniversary of each authorisation, the destruction of the results of surveillance operations has been considered
- At the fifth anniversary of each authorisation the destruction of the forms of authorisation, renewal or cancellation has been considered.

4.7.4 The Monitoring Officer will:

- Monitor the authorisations to ensure correct procedure has been followed
- Receive and investigate complaints by members of the public who reasonably believe they have been adversely affected by surveillance activities carried out by the Council.

4.7.5 The Office of Surveillance Commissioners has a duty to keep under review the exercise and performance of the Council of its surveillance powers. The Office of Surveillance Commissioners will regularly inspect the Council and may carry out spot checks unannounced.

4.8 **Refusals**

All refusals to grant authority to undertake Directed Surveillance must be recorded and retained for inspection.

4.9 **Breach of RIPA**

4.9.1 Evidence gathered where RIPA has not been complied with may not be admissible in Court and could lead to a challenge under Article 8 of the Human Rights Act.

4.9.2 Any perceived breach of this policy or the RIPA procedures should be reported to the Monitoring Officer in order that he/she may notify the Chief Surveillance Commissioner immediately (see following).

5. The use of a Covert Human Intelligence Source (CHIS)

The Council does not generally use a CHIS and any request to do so should be referred to the Solicitor of the Council in the first instance for guidance and advice. Further guidance is contained in the relevant Code of Practice.

There is no use of CHIS merely because a person offers information to the local authority that may be material to the investigation of an offence, but there would be if the authority asks the person to obtain further information.

5.1 The use of Covert Human Intelligence Sources

The same requirements of necessity and proportionality exist for the granting of authorisations for the conduct and use of a CHIS but the directed surveillance crime threshold does not apply. The Investigating Officer must obtain a unique reference number (URN) from the Solicitor to the Council and complete the Home Office approved application form (available on the Council's Intranet).

5.2 Authorising a CHIS

5.2.1 T**he authorisation must be *necessary*** on the same ground as for directed surveillance, for the purpose of preventing or detecting crime or preventing disorder. Secondly, **the authorised conduct or use of the source must be proportionate to the goal sought**. In this connection, and on the question of proportionality, it may be considered that the chances of collateral intrusion are particularly significant in the case of the use or conduct of CHIS. The Home Office Code of Practice recommends that the application includes a risk assessment for collateral intrusion.

5.2.2 **From 1st November 2012 the authorisation process for use of a CHIS has been subject to judicial approval meaning that any authorisation granted will require the approval of a Justice of the Peace, which necessitates making an application to the Magistrates Court. (See paragraph 3.6 for further detail).**

5.2.3 The Authorising Officer must be satisfied that arrangements exist for the proper oversight and management of the source that satisfy the requirements of section 29(5) of the Act and such other requirements as may be imposed by order made by the Secretary of State.

5.3 Covert Human Intelligence Sources may only be authorised if the following arrangements are in place:

Section 29(5) requires:

5.3.1 that there will at all times be an officer within the local authority who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security and welfare (section 29(5)(a));

5.3.1 that there will at all times be another officer within the local authority who will have general oversight of the use made of the source (section 29(5)(b));

5.3.2 that there will at all times be an officer within the local authority who has responsibility for maintaining a record of the use made of the source (section 29(5)(c));

5.3.3 that a risk assessment must be undertaken before authorisation;

5.3.4 that the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.

(The current regulations are The Regulation of Investigatory Powers (Source Records) Regulations 2000). These particulars are:

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the authority maintaining the records;

(d) the means by which the source is referred to within each relevant investigating authority; any other significant information connected with the security and welfare of the source;

(e) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(f) the date when, and the circumstances in which, the source was recruited;

(g) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the Act (see bullet points above) or in any order made by the Secretary of State under section 29(2)(c);

(h) the periods during which those persons have discharged those responsibilities;

(i) the tasks given to the source and the demands made of him in relation to his activities as a source;

(j) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(k) the information obtained by each relevant investigating authority by the conduct or use of the source;

(l) any dissemination by that authority of information obtained in that way;

(m) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority; and

(n) that records maintained by the local 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.

5.3.6 It is important to realise that it may well be a member of staff who becomes the source, depending on the manner of working used. It is not only persons outside the employ of the local authority who may be used as a source. If it is intended to make use of CHIS, then appropriate and specific training should be arranged for the officers responsible for the functions under section 29(5) (a) to (c) of the Act and also for any officer of the Council who is to be the CHIS.

5.4 **Juveniles and vulnerable persons as CHIS.**

This is governed by the Regulation of Investigatory Powers (Juveniles) Order 2000. Authorisation of juvenile or vulnerable CHIS may only be undertaken by the Head of Paid Service or his deputy in his absence.

5.5 **Judicial Approval of CHIS authorisations**

5.5.1 The Protection of Freedoms Act 2012 amended RIPA 2000 to make local authority authorisation of a CHIS subject to judicial approval. The change means that local authorities need to obtain an order from a Justice of the Peace, approving the grant or renewal of an authorisation, before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

5.5.2 **This new judicial approval mechanism is in addition to the existing authorisation process. The requirements to internally assess necessity and proportionality, complete the RIPA authorisation/application forms and seek approval from an Authorising Officer remain. Therefore, there is a two-stage process. First, an authorisation must be obtained from an Authorising Officer. Secondly, approval of the authorisation must be obtained from a Justice of the Peace. This involves applying to a Magistrates Court.**

5.5.3 A Justice of the Peace will only give approval to the granting of an authorisation for use of a CHIS if they are satisfied that:

- at the time the Authorising Officer granted the authorisation, there were reasonable grounds for believing that the authorisation was necessary and that the activity being authorised was proportionate, that arrangements existed that satisfied section 29(5) (see paragraph 3.3), that the Authorising Officer was a designated person for the purposes of section 29 of RIPA, that the grant of the authorisation was not in breach of

any restrictions imposed by virtue of section 29(7)(a) or 30(3) of RIPA, that any other conditions provided for by any Order were satisfied; and

- that there remain reasonable grounds for believing that the necessary and proportionate tests are satisfied and that any other requirements provided for by Order are satisfied.

5.6 CHIS Record Keeping

5.6.1 Records should be kept as prescribed by the Code of Practice (please see paragraph on Records and Documentation above). Where a source wearing or carrying a surveillance device is invited into residential premises or a private vehicle and records activity taking place inside those premises or vehicle, authorisation for use of that covert source should be obtained in the usual way.

5.6.2 The source should not use an invitation into residential premises or private vehicle as a means of installing equipment. If equipment is to be used other than in the presence of the covert source, an intrusive surveillance authorisation is necessary which **cannot** be granted by the local authority.

5.6.3 Home Office approved forms for the Review of a CHIS Authorisation; Renewal of a CHIS Authorisation and Cancellation of an Authorisation for the Use or Conduct of a CHIS are available on the Council's intranet.

6. Working with Other Agencies

6.1 When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this Policy and the Home Office approved application forms must be used and the agency advised of the Council's requirements. The agency must be advised, in writing, of what they are authorised to do.

6.2 When another agency including the Police (for example the Department for Work and Pensions or Trading Standards) wishes to use the Council's resources (for example officers or CCTV systems), that agency must use its own RIPA procedures and, **before** any officer agrees to allow the Council's resources to be used for the agency's purposes, the officer must obtain a copy of that agency's RIPA authorisation for the Council's central register.

7. Use of Social Media for Gathering Evidence

7.1 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 a RIPA authorisation is not usually required.

7.2 If it is necessary and proportionate for the Council to covertly breach access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if the relationship is established or maintained by the Officer (i.e. the activity is more than mere reading of the site's content). This could occur if an Officer covertly asks to become a 'friend' of someone on a social networking site.

8. Complaints

8.1 Procedure

The Council will maintain the standards set out in this Policy and the current Codes of Practice. The Chief Surveillance Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by the Act.

Contravention of the RIPA and/or Data Protection Act 1998 may be reported to the Information Commissioner at Chief Surveillance Commissioner Office of Surveillance Commissioners:

PO Box 29105
LONDON
SW1V 1ZU

Tel: 020 7035 0074
Fax: 020 7035 3114

However before making such a reference, any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the RIPA Monitoring Officer who will investigate the complaint.

A complaint concerning a breach of this Policy and Guidance document should be made using the Council's own internal complaints procedure. To request a complaints form, please contact the Solicitor to the Council:

Craven District Council
Council Offices
1 Belle Vue Square
Broughton Road
SKIPTON
BD23 1FJ

Tel: 01756 706325

This Policy together with the Codes of Practice published by the Secretary of State, are available at Craven District Council for consultation and reference. Copies of this Policy can be obtained from the Solicitor to the Council (address above). It is also available on the intranet.