BLACKBURN WITH DARWEN BOROUGH COUNCIL

PROCEDURAL GUIDE

FOR THE USE OF COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES ("CHIS")

NOVEMBER 2012
[reviewed by
Annual Overview
and Scrutiny
Committee
30/4/13]

To comply with the Regulation of Investigatory Powers Act 2000, Protection of Freedoms Act 2012, all its Regulations, Statutory Instruments, the Human Rights Act 1998 and having regard to the Codes of Practice and Additional Guidance to supplement the Codes published by the Secretary of State under S71(3)(a) of the Regulation of Investigatory Powers Act 2000

INDEX

A. GENERAL INTRODUCTION

1. This Procedural Guide, along with the statutory Codes of Practice published by the Secretary of State, must be readily available at Blackburn with Darwen Borough Council, Town Hall for consultation and reference by Investigating Officers, Members of the Council and the public and/or their representatives. These documents can be obtained from Legal Services

2. This Procedural Guide applies to any covert surveillance or use of CHISs by Blackburn with Darwen BC employees whose duties include investigation under properly delegated powers and by private investigators engaged to act as agents by those employees. It should be emphasised that the Regulation of Investigatory Powers Act 2000 (hereinafter referred to as RIPA) will only apply if the surveillance or use of CHIS is 'covert'; quite often such activities will be done overtly and so will fall outside RIPA so it is advisable to be familiar with the definition of 'covert' under RIPA as a starting point.

3. This Procedural Guide has been drafted specifically for Blackburn with Darwen BC and has regard to the provisions of the Codes of Practice and Addional Supplemental Guidance issued by the Secretary of State under S71 RIPA 2000. It should be noted that S72(1) RIPA states that a person exercising or performing any power or duty in relation to which provision may be made by a code of practice under Section 71 shall, in doing so, have regard to the provisions (so far as they are applicable) of every code of practice for the time being in force under that section. This Code has been compiled especially for Blackburn with Darwen BC only omitting elements which are not applicable to this Council. For example, there is no power of authorisation for 'intrusive surveillance' (see definition B7 in the Code) so references to such authorisations have been omitted. In addition, the authorisation forms for directed surveillance and CHIS are now separated as recommended by the Home Office.

4. All covert surveillance or use of CHISs should be authorised in writing and conducted in accordance with this Procedural Guide and should only be carried out if it is necessary for the purpose of preventing or detecting crime or of preventing disorder.

5. In addition covert surveillance and the use of CHISs should only be used by Blackburn with Darwen BC where it believes it is "proportionate" (see definitions section below).

6. Before authorising covert surveillance Authorising Officers should take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (collateral intrusion) and take measures wherever practicable to avoid it. Similarly they should also be aware of the possibility (though rare) of obtaining confidential information and take measures to avoid it. If there is a risk of

obtaining confidential material as defined in 83 of the definitions section below, it is necessary to obtain authorisation from a Chief Officer.

7. As far as surveillance is concerned this Procedural Guide is only concerned with 'directed' surveillance (see definitions below). This authority must not carry out 'intrusive surveillance' unless the Police are involved and the surveillance is conducted by them in accordance with their authorisation procedure. All surveillance operations in which the surveillance is likely to be intrusive need prior authorisation by the Chief Constable of Police and can only be carried out in cases where it is for the prevention and detection of "serious crime" (see definition 814 in the Definitions section below).

8. There should be no situation in which an Investigating Officer has to engage in covert surveillance or using a CHIS without obtaining authorisation. Authorisation can be obtained orally in urgent cases. However, it should be noted that Section 80 of the Act provides that without an authorisation the actions of the public authority would not be unlawful under RIPA. However, such unauthorised covert surveillance or use of a CHIS could contravene Article 8 European Convention of Human Rights (the right to respect for one's private and family life) brought into force in the UK by the Human Rights Act 1998. Having an authorisation makes it less likely that the covert surveillance or use of CHIS could be held to breach the Human Rights Act 1998, or be challenged in the Courts because it then becomes **'lawful for all purposes'** (Section 27(1) RIPA 2000).

9. For the avoidance of doubt surveillance notified to the subject is not covert and does not fall within the provisions of RIPA. Also, if information is obtained in an overt way, for example, when an officer behaves as an ordinary member of the public making test purchases or when checks are made on labelling etc which can only be made when overtly looking or asking questions. Such actions are usually already authorised specifically by other legislation in any event.

10. Common-sense dictates that surveillance will not be undertaken from, for instance a property next door or nearby the subject's property, unless the person who occupies the premises from which the surveillance is to take place has been notified and their written consent obtained (do we need to specify the method i.e. in writing).

B. DEFINITIONS

1. Authorising Officer

An Authorising Officer must be of 'Director, Head of Service, Service Manager or equivalent.' grade Therefore for the purposes of this

Procedural Guide the Authorising Officer shall be an officer of one of those ranks who may be appointed by the Council at any particular time to hold the position of 'Authorising Officer' across the Council Departments within Blackburn with Darwen. A list of these nominated Authorising Officers accompanies this Policy.

2. Collateral Intrusion

Collateral intrusion is an integral part of the decision making process and should be assessed and considered very carefully by both applicants and Authorising Officers.

The Revised Codes state Collateral Intrusion is intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation such as neighbours or other members of the subject's family. Where possible, steps should be taken to mitigate collateral intrusion.

Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is 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.

Prior to and during any authorised RIPA activity, a risk assessment should take place to identify the likely intrusion into the subject and any collateral intrusion. Officers should take continuing precautions to minimise the intrusion where possible. The collateral intrusion, the reason why it is unavoidable and your precautions to minimise it will have to be detailed on any relevant application forms. This will be considered by the Authorising Officer.

Before authorising surveillance the Authorising Officer should take into account the risk of collateral intrusion detailed on the relevant application forms as it has a direct bearing on the decision regarding proportionality.

The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but you should weigh up the importance of the activity to be carried out in operational terms on the one hand and the risk of collateral intrusion on the other hand.

3. **Confidential Material**

This has the same meaning as is given to it in sections 98-100 of the Police Act 1997.

It consists of matters subject to legal privilege, confidential personal information, or confidential journalistic material:

- **matters subject to legal privilege** includes both oral and written communications between a professional legal adviser and his or her client or any person representing his or 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 personal information** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  - either to his or her physical or mental health; or

  - 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. It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

    - it is held subject to an express or implied undertaking to hold it in confidence; or

    - it is subject to a restriction of disclosure or an obligation of secrecy contained in existing or future legislation.

- **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.

Note: Any authorisation for directed surveillance or CHIS will require the authorisation of the Chief Executive (or in their absence his deputy) if it is likely that Confidential Material will be obtained.

4. **Covert**

This is defined in Section 26(9)(a) of the RIPA as follows:

'Surveillance is covert if and only if it is carried out in a manner that is calculated to ensure that the persons who are subject to the surveillance are unaware that it is or may be taking place'.

5. **Covert Human Intelligence Source ("CHIS")**

This is defined in S26(8) RIPA as follows:

'..a person is a CHIS **if**-

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

(b) he covertly uses such a relationship to obtain information or to provide access to any information 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.'

(RIPA also says that references to the use of a CHIS include inducing asking or assessing a person to engage in the conduct of a CHIS or to obtain information by means of the conduct of a CHIS)

6. **Directed Surveillance**

This is defined in Section 26(2) of the RIPA which says surveillance is directed if it is <u>COVERT</u> but <u>NOT INTRUSIVE</u> and is undertaken:

'(a) for the purposes of a specific investigation or specific operation;

(b) 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); and

(c) 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'.

Therefore, by way of a summary, it is covert surveillance which is planned in advance to further a particular investigation and which is likely to result in the obtaining of information about a person's private or family life.

7. Intrusive Surveillance

THIS CANNOT BE UNDERTAKEN BY LOCAL AUTHORITY

Section 26(3) states that intrusive surveillance is covert surveillance that:

'(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

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

However, Section 26(5) says that surveillance which

'(i) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; but

(ii) 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'.**

Therefore, to be intrusive it has to take place actually on the residential premises or in the private vehicle except (in both cases) if a surveillance device is used. Surveillance using a device which is not on the private premises or in a private vehicle can still be 'intrusive' if it consistently provides information of the same quality and detail as might be expected from a device placed on the private premises or in the private vehicle. (Strangely, though it may not apply to Council work, a tracking device placed on a private vehicle is not intrusive according to the RIPA).

8. **'Necessity'**

In order for an Authorising Officer to decide whether an authorisation is necessary it must fall within ground (b) which is set out in Section 28 sub-section 3 of the RIPA namely:-

(a) for the purpose of preventing or detecting crime;
(b) the authorising officer describes why it is necessary to use covert surveillance in an investigation.

The Authorizing Officer should describe why it is necessary to use covert surveillance in an investigation. Since 1 November 2012, amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence sources)Order 2010 mean that a Local Authority can now only grant an authorisation under RIPA for the use of directed surveillance where the criminal offence being investigated attracts a maximum custodial sentence of six months or more, or is a criminal offence relating to the underage sale of alcohol or tobacco under sections 146 (sale of alcohol to children), 147 (allowing the sale of alcohol to children) or 147A (persistently selling alcohol to children) Licensing Act 2003 or Section 7 Children Act 1933 (sale of tobacco, etc, to persons under the age of 18 years).

9. **Private Information**

This is defined in the Act as including, 'in relation to a person', any information relating to his or her private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information.* This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a *public authority* of that person's activities for future consideration or analysis.

10. **Private Vehicle**

This is defined in the Act as any vehicle used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it (from the latter, paying passengers are excluded). From the point of view of a paying passenger therefore, the vehicle is **not** private.

11. '**Proportionate'**

If the proposed surveillance activity are deemed necessary, the person granting the authorisation must also believe that these actions are proportionate to what is sought to be achieved by carrying them out. There is no statutory definition of proportionality for covert surveillance or use of CHIS. However, the Code of Practice does provide some guidance. it should be noted that an authorisation will not be proportionate if it is excessive in the overall circumstances of the case. It should also be noted that RIPA must not be used in cases where other more open methods of investigation will suffice. This is a very important concept and all relevant officers should be aware of it.

The following elements should be considered:

1. Such methods must also only be used in cases where they are likely to result in the gathering of cogent (compelling or convincing) evidence.

2. Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence.

3. explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

4. considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, or obtaining the necessary result.

5. evidencing, as far as practicable, what other methods had been considered and why they were not implemented.

6. It is about balancing the seriousness of the crime being investigated and the threat to the general public against the interference with the privacy of the individual concerned.

7. Interference with a person's right to privacy will not be justifiable if the means used to achieve the aim are excessive in all the circumstances.

8. For example, it could be justified on the ground that there may be no other way of obtaining the evidence or perhaps a short period of surveillance could be justified on the grounds that it would be a quicker and most effective way of obtaining evidence.

9. The risk of collateral intrusion should also be considered when looking at proportionality as a high risk of this may tip the balance in favour of not using surveillance at all unless the risk can be minimised satisfactorily.

10. The degree of intrusion on the target and others.

12. RIPA Monitoring Officer

Blackburn with Darwen BC's RIPA Monitoring Officer is the Deputy Council Solicitor.

The RIPA Monitoring Officer:

- Will maintain a central record of all RIPA authorisations, renewals and cancellations.
- Will ensure that all applications for the use of directed surveillance are listed before a Magistrate as soon as practicable following the receipt of an authorised application;
- Will review the authorisations/renewals made on a regular basis to ensure that such authorisations/renewals are made properly, are appropriate and that all forms have been fully completed.
- Will also raise RIPA awareness within the Council.
- Will hall be prepared to advise, train and assist the Council's officers to enable them to comply with RIPA 2000.

13. Residential Premises

Section 48 subsection (1) provides that 'residential premises' mean (subject to subsection (?)(b)) so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used). RIPA states that the words 'residential premises' do not include a reference to so much of any premises as constitutes any common area to which the resident has access in connection with his use or occupation of any accommodation (Section 48(7)(b) RIPA). Therefore, surveillance from a common area is technically not intrusive, but there may be a higher risk of obtaining private information about someone so this must be considered when deciding whether or not to authorise the surveillance. For example, the entrance hall, stairs and lift in a block of flats is not counted as residential premises and this is important when assessing whether surveillance is intrusive or not.

14. Senior Responsible Officer (SRO)

Blackburn with Darwen BC's Senior Responsible Officer is listed in the Executive Director – Resources and Transformation. In

accordance with the Codes of Practice, the SRO is responsible for the following areas:

a) The integrity of the process in place within the Council for the management of Covert Human Intelligence Sources and Directed Surveillance
b) Compliance with Part II of RIPA and the Codes of Practice
c) Oversight of the reporting of errors to the relevant oversight commissioner
d) Engagement with the Commissioners and inspectors when they conduct their inspections
e) Ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports by the Officer of the Surveillance Commissioner.

15. **Subjects**

A member of the public or group thereof in respect of whom surveillance or the use of a CHIS has been authorised and such observed contacts of that individual or group of individuals as may come to notice during the course of the authorised surveillance or the use of a CHIS.

16. **Surveillance**

This is defined in the Regulation of Investigatory Powers Act 2000 (i.e. the RIPA) as including:

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

(b) recording anything monitored, observed or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device.

17. '**Surveillance Device'**

This is defined in Section 48(1) of RIPA as meaning 'any apparatus designed or adapted for use in surveillance'.

This therefore includes cameras, video cameras, listening and recording devices etc.

C. AUTHORISATIONS

1. Application

The whole of this section applies to directed surveillance (see definition number 5 above) and use of a CHIS (see definition number 4 above).

2. Authorisations

Authorisations or renewals of authorisations must be given by the Authorising Officer (see definition number 1 above) in writing. At the time an authorisation is given the Authorising Officer should look ahead to a suitable review date and specify this on the application form.

Once an authorisation is granted the Authorising Officer must ensure that the original forms are forwarded to the Surveillance Monitoring Officer. Surveillance cannot commence until the Authorised Application has been considered and granted by a Magistrate. The Surveillance Monitoring Officer will provide the applicant with a Unique Reference Number for the Application and will make arrangements for the Authorised Application to be heard as soon as practicable by the Magistrate.

3. Requirements

Before giving authorisation for surveillance or the use of a CHIS the Authorising Officer must be satisfied that:

(a) it is necessary for the purpose of preventing or detecting and complies with the statutory legal requirements in terms of maximum custodial sentence (see definition 9 above).

(b) it is necessary in that particular case, i.e. that particular case merits the use of this method of detection over other more open methods e.g. if it is a case where a person is suspected of having committed a crime like theft, justify why is this covert method of detection is necessary to obtain the evidence over other methods

(c) it is proportionate (see definition 11 above) to the seriousness of the crime or the matter being investigated and the history and character of the subject concerned. Balance the likelihood of obtaining private information against the seriousness of the crime being investigated.

(d) they have considered the degree of intrusion on the targets and others within their assessment and overt measures have been considered.

4. **Urgent Cases**

From 1st November 2012, there is no provision for the Council to use the urgent oral authorization.

5. **Time Limits**

Authorisations or renewals last three months beginning with the day upon which the authorisation or renewal takes effect. The length of time for surveillance or use of a CHIS to continue should be taken into account when deciding if it is proportionate or not.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further 3 month period.

Authorisation for the use and conduct of a CHIS last for 12 months.

It should be noted that the authorization time periods cannot be set to a shorter period within the time limits and must be controlled by the process of review, renewal and cancellation.

6. **Authorising Officer**

The Authorising Officer of the necessary standing in relation to surveillance or the use of a CHIS must be appointed by every department of Blackburn with Darwen BC which carries out investigatory functions and that name must be kept on records held by that department or/ and the Blackburn with Darwen BC Monitoring Officer.

7. **Reviews**

Reviews of the authorisation shall be carried out within a period of no longer than one month from the date of the authorisation or last review.

There are no requirements for a Magistrate to consider the review form.

Good practice suggests that a review should ideally be carried out after the first two sets of observations to determine if the allegation being investigated has been substantiated or seriously undermined. The Authorising Officer shall carry out the reviews and these reviews must not be confused with authorisations for renewal. The purpose of

a review is simply to decide whether or not the activity authorised should continue.

A review form should also be submitted to record changes in circumstances during the operation so that the Authorising Officer can have the opportunity to re-evaluate the operation in question. If however there are considerable changes to the nature of the operation in question to the techniques to be used during the operation then a new application should be issued and approval sought from the Magistrates.

8. Renewals

Renewals for either Directed Surveillance or CHIS application/authorisation must be approved by a Magistrate following authorisation from the Authorising Officer.

It is important to note that the renewal must be generated before the expiry of an authorization but such applications should not be made until shortly before the expiry of the original authorisation period is due to expire.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

9. Cancellation

The Authorising Officer must cancel an authorisation as soon as if he or she believes that the activity is no longer necessary or proportionate.

The Authorising Officer must formally instruct the investigating officer to cease the surveillance; it will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by the Surveillance Monitoring Officer.

All authorised applications must be cancelled as they do not naturally expire at the end of the authorisation period.

10. **Contents of Authorisation**

The written authorisation should specify

(1) names (where known) or descriptions of the subjects and any known history and character thereof;

(2) location of the subject and/or surveillance and (if relevant) the place where CHIS is to be located;

(3) the type of surveillance device or equipment to be used;

(4) the type of activities, numbers and names of officers who will be the CHISs (if relevant);

(5) that it is being undertaken for the purpose of preventing or detecting crime and that it fulfils the statutory legal requirements as detailed above

(6) that it is proportionate (see definition No.10 in the Definition Section above) i.e. specifying:

(a) the objectives of the surveillance, or the use of a CHIS;

(b) the crime or disorder being investigated (indicate the type of breach);

(c) the likelihood of obtaining private information about a subject or another person (collateral intrusion) and if the likelihood is high/medium /low, how that can be balance against the seriousness of the crime, so if the crime is not serious and there is a high likelihood of personal information being obtained it may not be proportionate to use this method of detection.

(7) Why it is necessary to use covert surveillance in the investigation

(8) The objectives of the activities;

(9) The name and nature of the investigation or operation and what makes the Authorising Officer believe surveillance or the use of a CHIS will achieve the objectives referred to;

(10) The length of time which should be proportionate to the wrong being investigated; and

(11) The risk of information relating to third parties' private and family life being obtained. This is known as 'collateral intrusion'.

(12) The likelihood of acquiring any confidential/religious material.

11. **Moving Subjects**

There may be a need to change the particulars if the subject moves and needs to be followed. An oral authorisation should be obtained as soon as reasonably practicable and a renewal form should be completed to reflect the change and this would be form R2. This may also apply where one subject is joined by a further person who needs to be watched for whom authorisation has not been obtained. Oral authorisation must be obtained as soon as reasonably practicable and the name added by means of a further application and authorisation if a longer period is required or it becomes clear a separate investigation is warranted.

12. **Covert Human Intelligence Sources (CHISs)**

A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as sources.

Under section 26(8) of the 2000 Act a person is a source if:

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

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.

By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above 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.

13. Conduct and Use of a Source

The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

The **conduct of a source** is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfill whatever tasks are given to them or which is incidental to it. **The Use and Conduct require separate consideration before authorisation.**

When completing applications for the use of a CHIS you are stating who the CHIS is, what they can do and for which purpose

When determining whether a CHIS authorisation is required consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

14. Management of Sources

Within the provisions there has to be;

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare **(Handler)**

(b) at all times there will be another person who will have general oversight of the use made of the source **(Controller)**

(c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

The **Handler** will have day to day responsibility for:

1. dealing with the source on behalf of the authority concerned;
2. directing the day to day activities of the source;
3. recording the information supplied by the source; and
4. monitoring the source's security and welfare;

5. The Controller will be responsible for the general oversight of the use if the source.

15. Tasking

Tasking is the assignment given to the source by the Handler or Controller by, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

Should a CHIS authority be required all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice

16. Management Responsibility

Blackburn with Darwen BC will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

The Handler of the source will usually be of a rank or position below that of the Authorising Officer.

It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be necessary the CHIS Codes of Practice should be consulted to ensure that the Council can meet its management responsibilities.

17. Security and Welfare

The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely

consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

18. Records Relating to the CHIS

These must contain the following by reason of the Regulation of Investigatory Powers (Source Records) Regulations 2000:

(a) the identity of the CHIS;

(b) the identity, where known, used by the CHIS (i.e. his or her 'alias');

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

(d) the means by which the CHIS is referred to within each relevant investigating authority (i.e. his or her 'code name');

(e) any other significant information connected with the security and welfare of the CHIS;

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

(g) the date when, and the circumstances in which, the CHIS was recruited; (or if already employed by the Council and allocated this task);

(h) the identities of the authorising officer and the applicant;

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

U) the tasks given to the CHIS and the demands made of him or her in relation to their activities as a CHIS;

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

(l) the information obtained by each relevant investigating authority by the conduct and use of the CHIS;

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

(n) in the case of a CHIS who is not an under-cover 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 CHIS activities for the benefit of that or any other investigating authority.

Therefore, the officer in charge of maintaining a record of the use of each CHIS should record all these details. The way these records are kept is designed to try to keep the CHIS safe from discovery by the subjects and safe from any harm which could result from their disclosure and also to keep in the open any money or other benefits paid to a CHIS who is not an employee or officer of an authorising body

D. RECORDS AND REPORTING

1. Copies of all written authorities and reviews should be kept for a period of 3 years after the conclusion of any Court proceedings arising for which the surveillance or use of the CHIS was relevant or until the next visit by the Assistant Surveillance Commissioner whichever is the later. In addition, copies of such records should be retained until 3 years after any OSC inspection.

2. Oral authorisations should be recorded as soon as reasonably practicable after being granted and kept in as 01 above.

3. For ease of monitoring the Surveillance Monitoring Officer whose job it is to keep all original application forms and any other RIPA forms in a special file and review them from time to time to make sure they are being completed properly and to meet the Assistant Surveillance Commissioner when he visits to inspect the forms. Also this officer shall be prepared to advise, train and assist the Council's officers to enable them to comply with RIPA 2000.

4. All information obtained during surveillance should be recorded by means of a surveillance log. This is a form which can be filled in which gives an account of the events observed and conversations heard at particular times which are recorded on the form or log. These should be kept as in 01 above.

5. All reviews of authorisations must be done in writing and kept as in 01 above as must grounds for withdrawal of authorisation or refusal to renew.

6. At no time must any of the recorded information be disclosed or used except for the purposes for which it was gathered at the time and for use in any future civil or criminal proceedings brought by or against the Council.

7. All information obtained by the CHIS and by the officer responsible for recording the use of the CHIS should be recorded by means of a daily log similar to the surveillance log referred to in 3. above.

8. Such records referred to in 6. above which also reveal the name(s) of the CHIS should only be disclosed if legally necessary or if desired by any Court.

9. Under the Revised Codes of Practice, Blackburn with Darwen BC should provide Elected Members from the Corporate Resources Overview and Scrutiny Committee with internal reports on the use of RIPA for them to consider at least on a quarterly basis. The Councillors should not, however be involved in making decisions on specific authorizations. There is a requirement that the identity of any subjects of authorized surveillance should not be identifiable in material reported to Elected Members.

10. The Executive member would approve the policy on an annual basis and the Corporate Resources Overview and Scrutiny Committee can ensure that the revisions that have been included are fit for purpose.

11. The Corporate Resources Overview and Scrutiny Committee should review the authority's use of RIPA, ensure that the policy is fit for purpose and set the policy at least once a year.

E. COMPLAINTS

Any complaints about any powers covered by this Procedural Guide can either be made under the Council's existing internal complaints system or to the Investigatory Powers Tribunal set up under S65 RIPA 2000.

F. 1 FORMS FOR DIRECTED SURVEILLANCE

R1/DS Application for authorisation, authorisation form and record of grant of oral authorisation

R2/DS Review form

R3/DS Application for renewal of authorisation and renewed authorisation

R4/DS Cancellation form

F. 2 FORMS FOR COVERT HUMAN INTELLIGENCE SOURCES

R1/CHIS Application for authorisation, authorisation form and record of grant of oral authorisation

R2/CHIS Review form

R3/CHIS Application for renewal of authorisation and renewed authorisation

R4/DS Cancellation form

F. 3 FORMS FOR DIRECTED SURVEILLANCE AND CHIS

R5/DS/CHIS Authorisation control sheet for both directed surveillance and CHIS's

For the sake of ease of reference these are named forms R1-5. If it is for directed surveillance it has the initials OS after the R, if for a CHIS it has CHIS.

1. **The application**

R1, the **main application form,** should be completed by the Investigating Officer who wants to apply to the Authorising Officer for authorisation in every case.

2. R1 must also be read and signed by the Authorising Officer and completed by him and signed when authorisation has been granted.

3. The application for **renewal** of authorisation R3 should be completed by the Officer in cases where written authorisation is about to end should it be necessary and proportionate to carry on the surveillance or use of CHIS beyond the time when it is due to end. R3 should then be completed by the Authorising Officer.

4. The review form R2 should be completed by the Authorising Officer at regular intervals of his own choosing or whenever the surveillance which has been authorised continues longer than one month. This is where the authorisation control sheet R5 is useful as evidence that reviews have been carried out.

5. A cancellation form R4 should be completed in all cases where the Authorising Officer considers that the directed surveillance or use of CHIS is no longer necessary or proportionate.

6. The authorisation control sheet R5 is essential as a monitoring tool for the authorising officer.

G. SEEKING AUTHORISATION FROM THE MAGISTRATES COURT

1. To authorise the use of Directed Surveillance and the use of a CHIS Blackburn with Darwen Borough Council will need to obtain an order approving the grant or renewal of an authorisation from a Magistrate or District Judge at the Magistrates Court before it can take effect.

2. If the Magistrate is satisfied that the statutory tests have been met and the use of the technique is necessary and proportionate an order will be issued approving the grant or renewal for the use of the technique as described in the application.

3. The flowchart at Annex A outlines the procedure for applying for Magistrate approval.

RIPA AUTHORISING OFFICERS

Senior Responsible Officer-Executive Director Resources and Transformation

Head of Public Protection-authorising officer
Audit and Assurance Manager-authorising officer

Quality control reviewing Officers [prior to submission of applications to authorising officers above]:
Group Manager-Consumer Protection
Principal Audit and Assurance Officer [Counter Fraud]

Surveillance Monitoring Officer- Deputy Head of Legal Services

Unique Reference Number

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

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

Unique Reference Number

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
• Name: • Address: • DOB: • Other information as appropriate:
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

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

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (512010 No.521).*

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

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

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

Describe precautions you will take to minimise collateral intrusion.

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?
10. Confidential information [Code paragraphs 4.1to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Unique Reference Number

11. Applicant's Details

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

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

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

13. Explain why you believe the directed surveillance is necessary [Code paragraph 3.3].

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

Unique Reference Number

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

Date of first review	

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

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

[Unique Reference Number

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

Name (Print)		Grade/ Rank		
Signature		Date and Time		

Urgent authorisation Expiry date:		Expiry time:	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June pt expires 4.59pm on 4th June		

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Public Authority *(including address)*	

Applicant		Unit/Branch /Division
Full Address		
Contact Details		
Operation Name		Operation Number* *Filing Ref
Date of authorisation or last renewal		Expiry date of authorisation or last renewal
		Review Number

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	Date

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

Unique Reference Number

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

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

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

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

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

Unique Reference Number

Signature

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

9. Authorising Officer's Statement.

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

Name (Print) Grade / Rank

Signature Date

10. Date of next review.

Unique Reference Number

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Authority *(including full address)*	

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

Details of renewal:

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

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

Unique Reference Number

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

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

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

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

7. Applicant's Details			
Name (Print)		Tel No	

Unique Reference Number

Grade / Rank

Date

Signature

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

9. Authorising Officer's Statement.

I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing.

This authorisation will be reviewed frequently to assess the need for the authorisation to continue.

Name (Print) Grade / Rank

Signature Date

Renewal From: Time: Date:

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

j Unique Reference Number

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

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

Details of cancellation:

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

Unique Reference Number

2. Explain the value of surveillance in the operation:

3. Authorising officer's statement.

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

Name (Print) Grade

Signature Date

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

Date: Time:

5. Authorisation cancelled. Date: Time:

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

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

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

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

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

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1] *Where appropriate throughout amend references to the Order relevant to your authority.*
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the purpose for which the source will be tasked or used.
4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.
5. Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (eg. 512010 No. 521).*
• In the interests of national security; • For the purpose of preventing or detecting crime or of preventing disorder; • In the interests of the economic well-being of the United Kingdom;

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

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

- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

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

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

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

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

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

9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.14).
10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means [Code paragraphs 3.3 to 3.5]?
11. Confidential information [Code paragraphs 4.1 to 4.21] Indicate the likelihood of acquiring any confidential information.
References for any other linked authorisations:

12. Applicant's Details.

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

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

Date

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] THE AUTHORISATION SHOULD DENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.

14. Explain why you believe the conduct or use of the source is necessary [Code paragraph 3.2] Explain why you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement [Code paragraphs 3.3 to 3.5].

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

16. Date of first review:	

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

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

18. Authorising Officer's Details

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

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

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

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

21. Authorising Officer of urgent authorisation

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

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

Unique Operation Reference Number* (*Filing Ref)

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

Review of a Covert Human Intelligence Source (CHIS) Authorisation

Public Authority *(including full address)*	

Applicant		Unit/Branch
Full Address		
Contact Details		
Pseudonym or reference number of source		
Operation Name		Operation Number* *Filing Ref
Date of authorisation or last renewal		Expiry date of authorisation or last renewal
	Review Number	

Unique Operation Reference Number* (* Filing Ref)

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	Date

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

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

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

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

Unique Operation Reference Number* (*Filing Ref)

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

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

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

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

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE,NOT THE TRUE IDENTITY.	
Name (Print)	Grade / Rank
Signature	Date

Unique Operation Reference Number* (*Filing Ref)

Date of next review:

Unique Operation Reference Number* (* Filing Ref)	

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

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

(Please attach the original authorisation)

Public Authority *(including full address)*	

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

Details of renewal:

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

Unique Operation Reference Number* (*Filing Rei)	

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

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

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

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

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

Unique Operation Reference Number* (*Filing Ref)	

use of the source.

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

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

9. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

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

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

Unique Operation Reference Number* (*Filing Ref)	

Name {Print)		Grade / Rank
Signature		Date
Renewal From:	Time:	Date: End date/time of the authorisation

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

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

Unique Operation Reference Number* (*Filing Ref)

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

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

Public Authority *(including full address)*	

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

Unique Operation Reference Number* (*Filing Ref)

Details of cancellation:

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

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

3. Authorising officer'S Statement. THIS SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

Name (Print) Grade

Signature Date

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

Date: Time:

RIPA AUTHORISATION SPREADSHEET
BLACKBURN WITH DARWEN BOROUGH COUNCIL

Type	Department	Date Authorised by	Likely to acquire	Title of investigation inc. desc & name of subjects	Urgency provs	Review dates		Renewals	Cancellations		Outcome
						Set by AO	Expiry		Set by AO	Expiry	

ANNEX A

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE

IN COURT HOURS

The local authority will contact Her Majesty's Courts and Tribunals Service (HMCTS) administration, who will schedule a hearing.

iocal authority representative will attend the hearing with the original:

- counter-signed RIPA aut orisation or notice form;
- the accompanying judicial application/order and;
- any other relevant reference material.

JP ensures that sufficient privacy is given to the hearing commensurate with the covert nature of the investigation (ie. no press, public, subject or legal representative present or court staff apart from Legal Adviser).

JPWill consider papers presented by local authority, asking r'ly additional questions in order to conclue whether an order to approve the grant of a RIPA authorisation or notice should be made. The papers by themselves make the case: It is not sufficient for the JP to rely solely on oral evidence where this is not reflected or supported by the form/papers.

-The local authority will call the court out of hours HMCTS legal staff who will ask for the basic facts and assess the urgency of the authorisation/notice. If the police are involved in the authorisation, the local authority will need to address why they cannot make the RIPA authorisation;

- If urgency is agreed, then HMCTS will arrange for local authority to attend a suitable location;

- Two copies of the forms arid supporting material should be available so that one set can be retained by the JP.

The JP must be satisfied that:

-there were 'reasonable grounds' for the local authgrity to believe the authorisation or renewal was both 'necessary' and 'proportionate', including whether all reasonable alternatives have been considered;

the reasqnable grounds as articulated by the local authority continue to apply and the authorisation/notice continues to be necessary and proportionate;

the local authority authorisation has been authorised by an appropriate designated person;

-there is no breach of any other restrictions imposed by order, see paragraphs 55-58, 72 73 and 83 of.this guidance.

efu toappfoJejH grant or renewal and quash the aufhdrisation or notice.

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

Approve the grant or renewabf the authorisation or notiCe.

-Tbe court must not exercise its i>6werto quah an authorisation or noticeunless.iHe applicant has bad at least 2 busin ss days from the date of the refusal in which to make representations.

gr tb; ; e0al 6f the RIPA authorisation or notice will not take effect and the local authority may not use the covert technique. Local authority may reapply addressing forexample; a technical error.

.recqnique may be used. Local 7 Gth rltY to resubmit any renewal or authorisation for the use of a different technique in this case.

Proxide loc uthority representative with a copy of 1he signed order and retu originaiHIPA form and any papers.
Legal Adviser or JP delivers copy order and authorisation to court admin office. Orders are kept securely and retained for 6 years.
Complete courthiudcopy court log [do NOT enter details on LIBRA].
ourtmgil}tain a copy of the court order and will send a yearly return to MOJ.