



**RHONDDA CYNON TAF**

# RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

***CORPORATE POLICY & PROCEDURES DOCUMENT***

**ON**

***THE REGULATION OF INVESTIGATORY-POWERS ACT***  
***2000 (RIPA)***

*POWERS ACT 2000 (RIPA)*

Christopher B Jones  
Director of Legal and Democratic Services,  
The Pavilions,  
Cambrian Park,  
Clydach Vale  
Tonypandy

**Adopted on:**

**Revised:**

**June 2005, September 2006, May 2007, May 2010,  
December 2010, February 2013, August 2014, ~~and~~ June  
2015 and October 2018**

## CONTENTS PAGE

	Page No
A Introduction and Key Messages .....	3
B Council Policy Statement	4
C Effective Date of Operation and Authorised Officer Responsibilities .....	5
D General Information on RIPA .....	5
E What RIPA Does and Does Not Do .....	6
F Types of Surveillance .....	6
G Conduct and Use of a Covert Human Intelligence Source (CHIS) .....	12
H <u>Online Covert Activity</u> .....	16
<u>I</u> Authorisation Procedures .....	18
<u>I-J</u> Working with / through Other Agencies .....	30
<u>J-K</u> Record Management .....	31
<u>K-L</u> Oversight of exercising of functions.....	33
<u>L-M</u> Concluding Remarks.....	34
Appendix 1 - List of Authorising Officer Posts	36
Appendix 2 – RIPA Flow Chart	38
Appendix 3 – Specific examples from Codes of Practice	39
Appendix 4 – RIPA A Forms-: Directed Surveillance	46
Appendix 5 – RIPA B Forms-: Covert Human Intelligence Source (CHIS)	65
Appendix 6 – Judicial Approval Forms	88

### **NB:**

The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding and application within Rhondda Cynon Taf County Borough Council, this Corporate Policy & Procedures Document refers to 'Authorising Officers'.

### **Acknowledgements:**

*The Council is most grateful to Birmingham City Council for their helpful contribution to the development of this Corporate Policy & Procedures Document.*

## A. Introduction and Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA') and Home Office's Code of Practices on "Covert Surveillance and Property Interference" and "Covert Human Intelligence Sources". The Council takes responsibility for ensuring the RIPA procedures are continuously improved.
2. The authoritative position on RIPA is, of course, the Act itself and the associated Home Office Codes of Practice and any Officer who is unsure about any aspect of this Document should contact, at the earliest possible opportunity, the Senior Responsible Officer, namely the Director of Legal and Democratic Services ('the Senior Responsible Officer') for advice and assistance. Appropriate training and development will be organised by the Service Director Senior Responsible Officer to relevant Authorising Officers and other senior managers.
3. The Codes of Practice are admissible as evidence in court. The provisions of the codes, if relevant, must be taken into account by the court.
4. Copies of this Document and related Forms will be placed on the Staff Intranet.
5. The Senior Responsible Officer will maintain and check the Corporate Register of all RIPA authorisations. It is the responsibility of the relevant Authorising Officer, however, to ensure the Senior Responsible Officer receives a copy of the relevant Forms as soon as practicable.
6. RIPA and this Document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This Document will, therefore, be kept under review by the Senior Responsible Officer and elected members. Authorising Officers must bring any suggestions for continuous improvement of this Document to the attention of the Senior Responsible Officer at the earliest possible opportunity.
7. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 1998/2018, General Data Protection Regulation 2018 and itsany associated Codes of Practice. RIPA ~~f~~Forms should be used where relevant and they will be only relevant where the criteria listed on the Forms are fully met.
8. If you are in any doubt on RIPA, this Document or the related legislative provisions, please consult the Senior Responsible Officer, at the earliest possible opportunity.

## **B. County Borough Council Policy Statement**

1. The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard the Senior Responsible Officer is duly authorised by the Council to keep this Document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administration and operational effectiveness, the Senior Responsible Officer is also authorised to add or substitute Officers authorised for the purpose of RIPA.
2. The Council's use of RIPA will be overseen by the Senior Responsible Officer, who is a member of the Corporate Management Senior Leadership Team.

## **C. Effective Date of Operation And Authorising Officer Responsibilities**

1. The Corporate Policy, Procedures and the Forms provided in this Document will become operative with effect from the date of its adoption by the Council. Prior to that, departments are encouraged to start using the Forms. After adoption, no other Forms will be allowable and any authorisations under the same will become null and void unless otherwise authorised by the Senior Responsible Officer. It is essential, therefore, that Chief Officers and Authorising Officers in their Divisions take personal responsibility for the effective and efficient operation of this Document.
2. Prior to the adoption date, and on subsequent revisions to this Document, Chief Officers have designated authorising officers within the appropriate divisions to take action under RIPA.
3. Authorising Officers will also ensure that staff who report to them follow this Corporate Policy & Procedures Document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this Document.
4. Authorising Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA ~~f~~Form unless, and until s/he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from his/her Service Director, the Council's Health & Safety Officer and/or the Senior Responsible Officer.
5. The Criminal Procedure and Investigation Act 1996 requires that any material, which is obtained during an investigation that may be relevant to the investigation, must be recorded and retained. Authorising Officers must ensure that any material obtained through directed surveillance or the use of a CHIS will be stored and disposed of in a secure manner and in compliance with Data Protection ActLegislation requirements.

6. Authorising Officers must also ensure that, when sending copies of any Forms to the Senior Responsible Officer (or any other relevant authority), the same are sent in sealed envelopes and marked 'Strictly Private & Confidential'.

#### **D. General Information on RIPA**

1. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires the County Borough Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, his home and his correspondence.
2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the County Borough Council may interfere in the citizen's right mentioned above, if such interference is:-
  - (a) in accordance with the law;
  - (b) necessary (as defined in this Document); and
  - (c) proportionate (as defined in this Document).
3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising covert surveillance and the use of a 'covert human intelligence source' ('CHIS') – e.g. undercover agents, in circumstances that are likely to result in the obtaining of private information about a person. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.
4. Directly employed Council staff and external agencies working for the Council are covered by ~~the Act~~RIPA for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorising Officers. Authorising Officers are those whose posts appear in Appendix 1 to this Document and duly added to or substituted by the Senior Responsible Officer.
5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the County Borough Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all involved with RIPA comply with this Document and any further guidance that may be issued, from time to time, by the Senior Responsible Officer.
6. A flowchart of the procedures to be followed appears at Appendix 2.

## **E. What RIPA Does and Does Not Do**

### **1. RIPA does:**

- require prior authorisation of directed surveillance;
- prohibit the Council from carrying out intrusive surveillance;
- require authorisation of the conduct and use of a CHIS;
- require safeguards for the conduct and use of a CHIS.

### **2. RIPA does not:**

- make lawful conduct which is otherwise unlawful;
- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.
- Apply in relation to covert surveillance activities that are unlikely to result in the obtaining of private information about a person.

3. If the Authorising Officer or any Applicant is in any doubt, she/he should ask the Senior Responsible Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

## **F. Types of Surveillance**

### **1. 'Surveillance' includes**

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- recording anything mentioned above in the course of surveillance. (*This would include filming, audio recording or writing down*)

~~surveillance, by or with, the assistance of appropriate surveillance device(s). (This would include use of binoculars or listening devices)~~

Surveillance may be conducted with or without the assistance of a surveillance device. (This would include use of binoculars or recording devices)

Note RIPA does not regulate the surveillance of places or premises per se, there has to be a human subject of the surveillance for RIPA to apply.

**Surveillance can be overt or covert.**

## Overt Surveillance

2. Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).
3. Similarly, surveillance will be overt if the subject has been told it will happen e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where a 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.

## Covert Surveillance

4. ~~Covert~~ Surveillance is Covert if it is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA).
5. RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

## Directed Surveillance

6. Directed Surveillance is surveillance which:-
  - is covert; and
  - is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance); and
  - is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
  - it is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain result in private information about an individual (whether or not that person is specifically targeted for purposes of an investigation). (~~Section 26(10) of RIPA~~).
7. Private information in relation to a person includes any information relating to his private and family life (Section 26(10) of RIPA). This includes 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, the fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the

obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. The use of the CCTV in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.
9. For the avoidance of doubt, only those Officers designated to be 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document are followed.

### **Intrusive Surveillance**

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

This is when it:-

- is covert;
- relates to residential premises and private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises/vehicle will be intrusive, where the device consistently provides information of the same quality and detail as might be expected to be obtained from a device inside the premises/vehicle.

11. Surveillance is intrusive when it:-

- is covert;
- relates to residential premises and private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises/vehicle will be intrusive, where the device consistently provides information of the same quality and detail as might be expected to be obtained from a device inside the premises/vehicle.

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



## 12. Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	<ul style="list-style-type: none"> <li>a) Police Officer or Parks Warden on patrol;</li> <li>b) Signposted or clearly visible Town Centre CCTV cameras (in normal use);</li> <li>c) Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists;</li> <li>d) Most test purchases (where the officer behaves no differently from a normal member of the public).</li> </ul>
Covert but not requiring prior authorisation	<ul style="list-style-type: none"> <li>a) CCTV or ANPR cameras providing general traffic, crime or public safety information.</li> <li>b) General observation duties forming part of the legislative functions of officers, as opposed to pre-planned surveillance of a specific person or group</li> <li>c) <u>Covert recording of a person voluntarily being interviewed by an officer during an investigation</u></li> </ul>
Directed (must be RIPA authorised-)	<ul style="list-style-type: none"> <li><u>a)</u> Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit;</li> <li><u>a)b)</u></li> <li><del>b)</del> Test purchases where the officer has a hidden camera or other recording device to record information if this is likely to include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner. <del>(NB When we use volunteers equipped with hidden cameras for undertaking underage sales test purchases we have developed procedures restricting where the camera films and the subsequent occasions when the film may be viewed and by doing so making the obtaining of private information very unlikely. In these circumstances we often consider that an authorisation is not necessary)</del></li> <li>c) CCTV or ANPR cameras used in a covert and pre-planned manner as part of a specific investigation</li> </ul>

Intrusive <b>(the Council cannot do this!)</b>	<ul style="list-style-type: none"> <li>a) Planting a listening or other device (bug) in a person's home, hotel room or in their private vehicle.</li> <li>b) Surveillance taking place at any prisons, police stations, high security psychiatric hospitals, lawyers' offices or court premises that are being used for legal consultations</li> </ul>
Directed but not intrusive	Surveillance of a communal stairway in a block of flats, an interview room, an hotel reception or dining area, a front garden of a premise readily visible to the public or a house used for a "house of horrors" type of operation
Neither <del>d</del> Directed or <del>i</del> Intrusive	<ul style="list-style-type: none"> <li>a) Use of a recording device by a CHIS where this is allowed by the CHIS authorisation;</li> <li>b) Overt or covert recording of a voluntary interview with a member of the public by a local authority officer</li> <li>c) Covert recording of noise nuisance where the recording device records only excessive noise levels</li> </ul>

Activity which should properly be authorised but which is not should be reported to the [Office of the Surveillance Investigatory Powers](#) Commissioner, in writing, as soon as the error is recognised.

The general observation duties of law enforcement officers including council officers do not require RIPA authorisation whether they are carried out covertly or overtly. Such general observation duties frequently form part of the legislative function of public authorities, as opposed to pre-planned surveillance of a specific person or group of persons. In effect these general observations would include officers parking in an area to keep an eye out or travelling around looking for what is going on.

Surveillance of persons while they are actually engaged in crime in a public place is not obtaining information about them which is properly to be regarded as 'private', so this does not require a ~~d~~Directed ~~s~~Surveillance authorisation.

Covert surveillance for any purposes other than for the prevention or detection of crime should be conducted under other legislation, if relevant, and RIPA authorisation should not be sought. This would include surveillance for the ordinary functions carried out by all authorities such as employment issues, investigating long-term sickness, contractual arrangements etc. The Council may only engage the use of RIPA when it is carrying out its "core functions" relating to enforcement. The disciplining of an employee is not such a core function, but if the investigation is for criminal misconduct the protection of RIPA is available as long as the activity is deemed to be necessary and proportionate.

If any covert activities do not require RIPA authorisation but, for instance, there is a possibility that some private information may be obtained unexpectedly, it would be

good practice for the officer to record in writing in advance the reasons why it is necessary and proportionate for the activities to take place. This will help to demonstrate that the officer has given consideration to relevant human rights issue. Similar considerations could apply if an elderly victim wanted a CCTV camera to be installed inside the house to protect the person from cold-callers. Officers would not be able to authorise this under RIPA because it would be intrusive surveillance but, as there are good reasons for installing the camera, a human rights consideration form should be used to record the reasoning.

If such human rights consideration forms are used to cover general use of certain covert techniques in a particular set of circumstances, such as for certain types of test purchasing activities, then the Authorising Officer should periodically review the use made of the technique, to check whether any significant collateral intrusion has occurred. If this has occurred the Authorising Officer must decide whether the particular technique should be allowed to continue or only allowed to continue after changes have been made.

The original versions of such general human rights consideration forms should be forwarded for inclusion in the Central Register, where they can be assessed by the Senior Responsible Officer.

DRAFT

## **G. Conduct and Use of a Covert Human Intelligence Source (CHIS)**

### **Who is a CHIS?**

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.
2. RIPA does not apply in circumstances where members of the public volunteer information to the County Borough Council as part of their normal civic duties, or to contact numbers set up to receive information.

### **What must be authorised?**

3. The Conduct or Use of a CHIS requires prior authorisation. Most authorisations will be for both conduct and use.
  - Conduct of a CHIS = these are the steps taken by the CHIS on behalf of the Council. They are actions establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information;
  - Use of a CHIS = these are the steps taken by the Council in relation to the CHIS. They are actions regarding inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place;
  - Establishing a relationship means setting it up; ~~and~~ maintaining a relationship ~~involves~~ means endurance of the relationship over a particular period. Repetition is not always necessary to give rise to a relationship, but whether one exists depends on the circumstances including the length of time of the meeting and the nature of any covert activity;
  - Unlike for ~~d~~Directed ~~s~~Surveillance that relates to the obtaining of private information, the conduct or use of a CHIS involves the covert manipulation of a relationship to gain any type of information.
4. The Council can use CHIS's IF, AND ONLY IF, RIPA procedures, detailed in this Document are followed.

### **Circumstances when authorisation is not required**

Not all human source activity will meet the definition of a CHIS. These include:

- Persons volunteering or providing information that is within their personal knowledge, without being induced, asked or tasked by the Council;
- Persons who are required to provide information out of a professional or statutory duty;
- Persons who are tasked to do something that does not involve them in a relationship with the target, such as recording what they observe.

Nevertheless Officers should keep under constant review such human sources, as well as members of the public who offer their services to assist an investigation, in order to decide whether, in their judgement, at some point the source needs to become a CHIS. This is to prevent “tasking by implication” where the source thinks they are being encouraged to obtain certain information and such tacit encouragement could amount to tasking the source as a CHIS. Tasking of a person should not be the sole benchmark in seeking a CHIS authorisation, as it is the activity of the CHIS in exploiting a relationship for a covert purpose that triggers authorisation. Therefore it is possible that a person will become engaged in the conduct of a CHIS without the Council inducing, asking or assisting the person to engage in that conduct.

Any manipulation of a relationship by the council is likely to engage the subject’s Article 8 right to privacy, regardless of whether or not the council intends to acquire private information. Consequently an authorisation will be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the Council.

### **Handler, controller and record keeper for CHIS**

5. It is important that both Officers and the CHIS are made fully aware of the extent and limits of any conduct authorised. The following persons must be nominated in relation to each CHIS:

#### **Handler**

This person must be an officer of the Council and that person will have day-to-day responsibility for dealing with the CHIS, for recording the information supplied by the CHIS and for monitoring the CHIS’s security and welfare. The Handler will need to explain to the CHIS what he or she must do. For example, the CHIS may be someone who assists a trading standards officer and is asked to undertake a test purchase of items that have been misdescribed.

#### **Controller**

This person must be an officer of the Council and that person will normally be responsible for the management and supervision of the handler as well as carrying out a general oversight of the use made of the CHIS. This person is likely to have general responsibility for the management of covert operations undertaken by the service.

The Controller and Handler should record that they have been briefed on the parameters of the use and conduct of the CHIS that has been authorised.

The day-to-day contact with the CHIS is to be conducted by the Handler. Some arrangements may be made in direct response to information provided by the CHIS on his meeting with the Handler. Before any person is authorised to act as a CHIS, the Handler should complete a **rRisk aAssessment fForm** for the person and the proposed activity. This may require contact with the police to find out if the proposed target is likely to pose a risk to the CHIS. Steps should be taken to protect the safety and welfare of the CHIS, when carrying out actions in relation to an authorisation, and to others who may be affected

by the actions of CHIS. Before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any action and the likely consequences should the role of the CHIS become known to the subject of the investigation or those involved in the activity which is being investigated. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

The Handler is responsible for bringing to the Controller's attention any concerns about the personal circumstances of the source, insofar as they might affect:

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

Where deemed appropriate, the Controller must ensure that the information is considered by the Authorising Officer, and a decision taken on whether or not to allow the authorisation to continue.

### **Tasking**

6. Tasking is the assignment given to the CHIS by the Handler or Controller, asking the CHIS to obtain, provide access or to disclose information. Authorisations should not be drawn so narrowly that a separate authorisation is needed every time the CHIS is tasked. Rather the authorisation should cover in general terms the nature of the CHIS's tasks, although a new authorisation might be needed if the nature of the tasks changes significantly. In those circumstances the matters should be referred to the Authorising Officer to decide whether a new authorisation is needed.

It is difficult to predict exactly what will happen when the CHIS meets the subject of the investigation and there may be occasions when unforeseen actions occur. When this happens the occurrence must be recorded as soon as practicable after the event. If the existing authorisation is insufficient it should either be updated at a review (for minor amendments only) or cancelled and a new authorisation should be obtained before any further activities are carried out.

### **Juvenile Sources**

7. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child who at that time is under 16 years of age be authorised to give information against his or her parents. Only the Head of Paid Service is duly authorised by the Council to use Juvenile Sources, as there are other onerous requirements for such matters.

### **Vulnerable Individuals**

8. A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

9. A Vulnerable Individual will only be authorised to act as a CHIS in the most exceptional of circumstances. Only the Head of Paid Service is duly authorised by the Council to use Vulnerable Individuals, as there are other onerous requirements for such matters.

### **Test Purchases**

10. Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. ~~For example, a~~ Authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).
11. By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop, if there is a likelihood of obtaining private information, will require authorisation as ~~d~~Directed ~~s~~Surveillance. A combined authorisation can be given for a CHIS and also ~~d~~Directed ~~s~~Surveillance.

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

12. Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) or non-verbal noise (such as music, machinery or an alarm) will not normally capture private information and, therefore, does not require authorisation. Also the recording of verbal content at a level which does not exceed that which can be heard from the street outside or adjoining the property with the naked ear, is unlikely to require authorisation, since the perpetrator would normally be regarded as having forfeited any claim to privacy.

When a member of the public is asked to keep a diary to support incidents of anti-social behaviour or noise they should be given detailed instructions in writing about what they are expected to do or not do and what information they are expected to record,. This will help to prevent them from, in effect, carrying out ~~d~~Directed ~~s~~Surveillance on behalf of the Council. These instructions should include telling the person not to attempt to obtain information covertly, for instance by asking questions of the targeted person, because if the person were to do so they could be acting as a CHIS on behalf of the Council. Authorising Officers should carry out random inspections of diary entries to ensure that a RIPA authorisation is not required.

13. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

## **Surveillance devices and other technical equipment**

14. A CHIS who is authorised to wear or carry a surveillance device, such as a recording device, does not require a separate ~~d~~Directed ~~s~~Surveillance authorisation, provided the device will only be used in the presence of the CHIS, even if this takes place inside a residential premise or private vehicle.
15. Each Division should maintain a register of all equipment that is used for surveillance work. This equipment could include surveillance vehicles, cameras, video recorders and binoculars. Specific individuals should be given responsibility for issuing the equipment from the Divisional central store or location. Every time each item of equipment is issued for surveillance purposes a record should be made of the following:
  - Identification of equipment;
  - RIPA authorisation number for which this equipment is being used;
  - Date the equipment was issued;
  - Person taking possession of the equipment;
  - Date the equipment was returned to the Divisional store.
16. If equipment is issued to a particular officer on a long-term basis where it might also be used for purposes other than covert surveillance, the officer should record on the equipment register any occasions when that equipment is being used for covert surveillance. For instance this could apply to the issuing of binoculars or a camera. However if equipment such as a camera is issued to an officer, but it is only used to record evidence and not for any covert purpose then there is no requirement for such equipment to be recorded on the register.
17. The Central Register held by the Senior Responsible Officer shall include details of surveillance equipment available within the Council, and in which Division this is held.

## **H. Social Networking Sites and Internet Sites Online Covert Activity**

~~1718.~~ The use of the internet may be required to gather information prior to and/ or during an operation, which may amount to directed surveillance. Therefore whenever officers intend to use the internet as part of an investigation they must first consider whether the proposed activity is likely to interfere with a person's Article 8 right to privacy, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of the specific case. Therefore when it is considered that private information is likely to be obtained an authorisation must be sought. In addition, when an officer wishes to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered.

~~1819.~~ Whilst it is the responsibility of an individual to set privacy settings to protect against unsolicited access to their private information on a social networking



site, and even though the data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. However repeat viewings of such open source data may constitute directed surveillance and this should be judged on a case-by-case basis.

~~1920.~~ 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 a 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.

~~201.~~ CHIS authorisation is only required when using an internet trading organisation such as E-Bay or Amazon Marketplace in circumstances when a covert relationship is likely to be formed. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at this stage.

1. The use of the internet may be required to gather information prior to and during the course of an operation. This activity may amount to Directed Surveillance and in some circumstances may also require a CHIS authorisation. Although the information or activity viewed is online rather than at a physical site, the officer must still consider a person's Article 8 right to privacy, collateral intrusion, and what activity is likely to be considered necessary and proportionate to meet the objectives of the specific case.
2. Much information on the internet can be accessed without the need for an authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if an officer repeatedly studies an online presence, or systematically extracts and records information, this may give rise to privacy issues and the necessary authorisation(s) will be considered.
3. Depending on the online platform in question and the privacy settings both available and set by the individual, there will be differing expectations of privacy. Where an individual or company places information on a publically accessible database, such as the telephone directory or Companies House there is unlikely to be a reasonable expectation of privacy; an officer may access this information without requiring an authorisation. If privacy settings have not been applied on social media platforms, there may still be a reasonable expectation of privacy over information on that platform.
4. If an officer interacts with a person online where the individual they are communicating with could not reasonably be expected to know their true identity (as an officer of the Council rather than a private individual), the officer must consider whether the activity requires a CHIS authorisation. Where a relationship is established or maintained for a covert purpose to obtain information, a CHIS authorisation is likely to be required.

5. Where a website or social media account requires a minimum level of interaction, such as sending a friend request before access is permitted, this may not of itself constitute a relationship. However, any further interactions of the officer once they have entered the website or social media account may require CHIS authorisation.
6. In determining whether authorisation for Directed Surveillance is required in relation to online activity, the officer will consider:
- Whether the investigation or research is directed towards an individual or organisation;
  - Whether it is likely to result in obtaining private information about a person or group of people;
  - Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
  - Whether the information obtained will be recorded and retained;
  - Whether the information is likely to provide an observer with a pattern of lifestyle;
  - Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
  - Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
  - Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.
7. The Codes of Practice under the Act provide a number of examples in relation to online covert activity; these are included in Appendix 3.

#### **HI. Authorisation Procedures**

1. Directed sSurveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. Appendix 2 provides a flow chart of process from application consideration to recording of information

#### **Authorisations**

An application for authorisation must be made on the Authorisation Form outlining:

- The activities to be authorised;
- The identities, where known, of those to be the subject of any eDirected sSurveillance;
- The purpose of the operation or investigation including a summary of the intelligence case for the operation. The intelligence case should give justification for each individual covert activity that the Applicant wishes to be authorised, eg a) watching a premise and b) following a vehicle;

- For the use of ~~d~~Directed ~~s~~Surveillance confirmation that the action proposed is for the purpose of preventing conduct that constitutes one or more criminal offences, one of which carries a maximum sentence of at least 6 months imprisonment (or is a specified offence under the Licensing Act 2003 or Children and Young Persons Act 1933 or the Children and Families Act 2014);
- For the use of a CHIS confirmation that the action proposed is intended to prevent or detect crime and/or disorder;
- A statement outlining why the operation is considered to be necessary;
- A statement outlining why the operation is proportionate to what it seeks to achieve;
- An explanation of the information which it is desired to obtain as a result of the authorisation and how obtaining this information will assist the investigation;
- An assessment of the potential for collateral intrusion - that is to say, interference with the privacy of persons other than the subjects of the operation - and the precautions to minimise such intrusion;
- An assessment of the likelihood of acquiring any confidential material and how that will be treated;
- ~~Where authorisation is sought urgently, the reasons why the case is considered to be urgent.~~

The need for an authorisation has to be judged at the time of the authorisation, not with the benefit of hindsight.

When authorising the conduct and use of a CHIS, the Authorising Officer should state that he or she is authorising a specific person, referred to by a pseudonym, to be a CHIS for the purpose of investigating the specified illegal activity. After this the Authorising Officer should state "The conduct of the CHIS identified as (pseudonym) that I authorise is as follows..." and then identify this conduct. A CHIS application is person specific, therefore this application must focus on the person who is to conduct the activity, not solely the operation.

Although there is no statutory requirement to do so, the process of judicial approval will be helped if the officer includes background information about the offences under investigation and the kind of evidence that is needed to prove the offences. This information can be provided via a separate background information document.

There must be a record of whether authority was given or refused, by whom and the time and date.

Once an authorisation has been granted the Applicant must ensure that all practitioners, both in the Council and in other agencies, are made aware of the extent and limitations of the authorisation, usually by means of a briefing from the Applicant.

On some occasions applications are made when the supporting information is not received from another enforcement agency such as the police, but instead it might be received from a concerned person or anonymously or from an aggrieved party. In these circumstances the Authorising Officer should view

the intelligence or other report to ensure that a potential CHIS relationship is not being developed.

Once the application has been authorised by the Authorising Officer the authorisation then needs to receive judicial approval from a magistrate (see below).

## **Reviews**

Authorising Officers should consider an appropriate frequency for the reviews at the start of the investigation. Each authorisation should be regularly reviewed to assess whether it remains necessary and proportionate for it to continue. This review should be recorded using the 'Review Form' outlining:

- The review number;
- Summary of the information obtained to date and its value;
- The reasons why it is still i) necessary and ii) proportionate to continue with the operation;
- Details of any incidents of collateral intrusion or the acquiring of confidential information.

Any proposed changes to the activities or targets of the operation should be brought to the attention of the Authorising Officer by means of a review. Authorising Officers should consider proportionality issues before approving or rejecting them. Where the original authorisation targeted unknown persons or associates, once they are identified a review should be carried out to include the identities of these individuals.

During a review the Authorising Officer may amend specific aspects of the authorisation, for example to cease surveillance against named persons or to discontinue the use of a particular method. Authorising Officers should also check whether Applicants are not making use of some of the tactics that have been authorised, where it might be case that some of the tactics are being requested out of habit rather than from necessity.

When reviewing the use of a CHIS the Applicant should include the use made of the CHIS during the period, the tasks given to the CHIS, the information obtained from the CHIS and the reasons why enforcement action is not possible at this stage.

## **Renewals**

The Authorising Officer who grants an authorisation should, where possible, be responsible for considering subsequent renewals of that authorisation and any related security or welfare issues. Any request for a renewal of an authorisation should be recorded using the Renewal Form outlining:

- Whether this is the first renewal, or on how many occasions it has been renewed;
- Details of any significant changes to the information given in the previous authorisation;
- The reasons why it is still i) necessary and ii) proportionate to continue with the operation;

- The content and value to the operation of the information so far obtained;
- The results of the regular reviews of the operation.

### **Cancellations**

Authorising Officers must cancel an authorisation if they are satisfied that the operation will no longer meet the criteria under which it was authorised. All authorisations must be cancelled in writing using the **Cancellation Form** outlining:

- The reason for the cancellation of the authorisation;
- The value of the authorised activities in the operation;
- Whether or not the objectives of the operation were achieved;
- The products of surveillance that were obtained (such as written notes, photographs, hard disc recordings or video footage) and how they will be stored or disposed of; (Any products of surveillance that do not match the objectives of the investigation should be disposed of as soon as possible, even if other material needs to be retained as part of the investigation.);
- The date and time when the Authorising Officer instructed the operation to cease;
- The date and time when the authorisation was cancelled;
- It is considered to be best practice for the Applicant to record each date that surveillance has been carried out under the authorisation in the box relating to the value of the authorised activities.

If the requirement for **Directed Surveillance** needs to continue for some time after the last surveillance activity etc has taken place, then an explanation for the delay in cancelling the authorisation should be included on the Cancellation Form. This explanation should show why it was necessary and proportionate for the surveillance to continue, for instance because an assessment needed to take place of the intelligence that was available.

When cancelling CHIS authorisations the Applicant should record whether technical surveillance equipment was used by the CHIS and, if so, state what information was recorded by the equipment.

After a CHIS authorisation has been cancelled the security and welfare of the CHIS should continue to be taken into account. Therefore the Authorising Officer will need to be satisfied that all welfare matters have been addressed.

### **Authorising Officers**

2. Forms can only be signed by Authorising Officers. Authorised posts are listed in Appendix 1. This Appendix will be kept up to date by the Senior Responsible Officer, and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Senior Responsible Officer for consideration, as necessary. The Senior Responsible Officer has been duly authorised to add, delete or substitute posts listed in Appendix 1.
3. Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal Schemes of Management.

RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. The authorisations do not lapse with time!

4. The Council and those persons acting under of the Act must have regard to the Codes of Practice issued under the Act. Each Authorised Officer will have access to copies of these codes which are available at [www.gov.uk](http://www.gov.uk). The Codes of Practice give some helpful examples to provide guidance on various points. Some of these examples are given in Appendix 3, but should be used with care, as it is not possible for theoretical examples to replicate the level of detail to be found in real cases.

### **Training**

5. It is a requirement that Propersuitable training ~~will~~ be given to Authorising Officers who are authorised to sign any RIPA Forms and also to Applicants.
6. If the Senior Responsible Officer feels that an Authorising Officer has not complied fully with the requirements of this Document, the Senior Responsible Officer is duly authorised to retract that Officer's authorisation.

### **Application Forms**

7. ~~For all Sections~~ Only the approved RIPA ~~f~~Forms set out in this Document must be used. Any other forms used will be rejected by the Authorising Officer and/or the Senior Responsible Officer.

### **'DS Forms' (Directed Surveillance) – See Appendix 4**

8. Form DS 1 Application for Authority for Directed Surveillance  
Form DS 2 Renewal of Directed Surveillance Authority  
Form DS 3 Cancellation of Directed Surveillance  
Form DS 4 Review of Directed Surveillance Authority

### **CHIS Forms – See Appendix 5**

9. Form CHIS 1 Application for Authority for Conduct and Use of a CHIS  
Form CHIS 2 Renewal of Conduct and Use of a CHIS  
Form CHIS 3 Cancellation of Conduct and Use of a CHIS.  
Form CHIS 4 Record of use of a CHIS.  
Form CHIS 5 Review of Conduct and Use of a CHIS

### **Grounds for Authorisation**

10. Directed Surveillance (DS Forms) can be authorised by the Council only on the following grounds:

For the purpose of preventing or detecting conduct which:-

- a. Constitutes one or more criminal offences;

AND

- b. At least one of the criminal offences is punishable, whether on summary conviction or on indictment, by a maximum term of imprisonment of at least 6 months of imprisonment;

OR

- c. Is an offence under Section 146, 147 or 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933 or Section 91 or 92 of the Children and Families Act 2014.
11. The Conduct and use of the Covert Human Intelligence Sources (CHIS Forms) can be authorised by the ~~County Borough Council~~ only ~~on the following ground:~~ ~~F~~for the purpose of preventing or detecting crime or of preventing disorder.

### **Necessary, Proportionate, Collateral Intrusion and Confidential Material**

12. **What does the term “necessary” mean?**

RIPA provides a framework for ensuring that any surveillance activities do not infringe the human rights of the individual. In considering whether to grant an authorisation, the authorising officer must consider whether the proposed conduct is necessary.

**An ~~a~~Authorising ~~e~~Officer must consider a number of issues in deciding if a proposed course of action is necessary. These include:**

- Balancing the “target’s” human rights with the rights and freedoms of other individuals;
- Deciding that the required information needs to be acquired in this way and that it cannot reasonably be acquired by other means that would involve less, or no, invasion of privacy.

Every case must be considered on its merits, as what is necessary in some circumstances is not necessary in others. Always consider other ways in which the information could be obtained, such as use of third party information powers, the Internet, and other sources. The information must be necessary in order to carry out the investigation. The Council should not consider obtaining information through covert means that it does not need for the investigation. ~~It might be nice to know and very interesting but if it is not strictly necessary to have it then officers should not seek to obtain it.~~ Officers need to show why it is necessary in this case and at this time.

### **What does the term “proportionate” mean?**

Proportionality is a very important concept, and it means that any interference with a person’s rights must be proportionate to the intended objective. This means that the action is aimed at pursuing a legitimate aim (for example, protecting a child from potential abuse). Interference will not be justified if the means used to achieve the aim are excessive in all the circumstances. Thus where surveillance is proposed that action must be designed to do no more than meet the objective in question; it must not be unfair or arbitrary; and the impact on the individual or group of people concerned must not be too severe.

Each action authorised should bring an expected benefit to the investigation and should not be disproportionate. The fact that a suspected offence may be serious will not on its own render intrusive actions proportionate. No action will be considered proportionate if the information sought could reasonably be obtained by other less intrusive means.

### **What questions should the Applicant address on the proportionality part of the aApplication fForm?**

The Applicant should address the following elements of proportionality:

- (a) Balance the size and scope of the proposed activity against the gravity and extent of the perceived offence;
- (b) Consider whether the activity is an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- (c) Explain how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- (d) Evidence, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Additionally, in respect of CHIS activity, the Applicant must address the following element of proportionality:

(e) whether the conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation.

### **What does the term “collateral intrusion” mean?**

Collateral intrusion occurs when officers obtain private information about people unconnected with the investigation. Authorising Officers must consider the likelihood and extent of collateral intrusion when considering any application and ensure that Applicants have planned to minimise collateral intrusion. Where the collateral intrusion is unavoidable the activity may still be authorised, provided that the collateral intrusion is considered to be proportionate. Situations where collateral intrusion can occur include where

- Observing how busy a business is, results in watching unconnected people come and go;
- At a test purchase, we might observe or overhear other customers' conversations.

Particular consideration must be given where confidential material may be involved.



## What does the term “confidential material” mean?

Confidential material is anything

- That is subject to legal privilege, for example communications between a legal adviser and his/her client;
- That is a communication between a Member of Parliament/ Assembly Member/ Member of European Parliament and a constituent regarding constituency matters;
- That is confidential personal information, for example information about a person’s health or spiritual counselling or other assistance given or to be given to him or her;
- That is confidential journalistic material (this includes related communications), that is, material obtained or acquired for the purposes of journalism and subject to an undertaking to hold it in confidence.

In cases where it is likely that knowledge of confidential material will be acquired, then the ~~d~~Directed ~~s~~Surveillance must be authorised by the ~~Chief Executive~~~~Head of Paid Service~~

### **Assessing the Application Form**

13. Before an Authorising Officer signs a Form, s/he must:-
- (a) Be mindful of this Corporate Policy & Procedures Document, the training provided and ~~any other guidance issued, from time to time, on such matters~~current guidance.
  - (b) Satisfy him/herself that the RIPA authorisation is:-
    - i) in accordance with the law;
    - (ii) necessary in the circumstances of the particular case on one of the grounds mentioned in paragraph 10 above; and
    - (iii) proportionate to what it seeks to achieve.
  - (c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information. **The least intrusive method will be considered proportionate by the courts.**
  - (d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (Collateral Intrusion). Measures must be taken ~~wherever practicable~~ to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;
  - (e) Set a date for review of the authorisation and review on or before that date;

- (f) Ensure that the ~~a~~Application ~~f~~Form has been identified with a Unique Reference Number that the Applicant has obtained from the ~~appropriate Co-ordinator in that service area~~office of the Senior Responsible Officer.

~~For directed surveillance the URN will be of the format of a prefix followed by a number that increases by 1 with every application eg C001, C002. The prefixes used will be as follows:~~

~~Corporate Services — C  
Counter Fraud Team — F  
Public Health & Protection — P  
Regeneration & Planning — R  
Streetcare — S~~

~~For the use of a CHIS the URN will be of the format of the appropriate prefix followed by CHIS followed by a number that increases by 1 with every application e.g. PCHIS001, PCHIS002.~~

~~For ~~d~~Directed ~~s~~Surveillance, the URN will follow the format:~~

- ~~• RCT/001/18/DS~~

~~Where 001 is a sequentially progressive number, 18 identifies the current year and DS indicates the application as relating to Directed Surveillance.~~

~~For the use of a CHIS, the URN will follow the format:~~

- ~~• RCT/001/18/CHIS~~

~~Where 001 is a sequentially progressive number, 18 identifies the current year and CHIS indicates the application as relating to CHIS activity and authorisation.~~

- (g) ~~Each Division will keep a register of the RIPA authorisation / review / renewal / cancellation / rejection forms completed within the Division and ensure that the Divisional RIPA Register is duly completed, and that a copy of the RIPA Forms (and any review / renewal / cancellation / rejection of the same) is included on the Divisional Register. The original RIPA authorisation (and any review / renewal / cancellation / rejection of the same) form shall be forwarded to the Senior Responsible Officer's Central Register, as soon as practicable. Completed RIPA documentation, including applications, authorisations, rejections, renewals and cancellations, shall be forwarded in good time to the office of the Senior Responsible Officer for filing and updating the Central Register. This shall not preclude the individual Division maintaining a copy of the documentation for live operational activity purposes.~~
- (h) The Authorising Officer should also record whether or not they are directly involved in the investigation. (NB an Authorising Officer should not be responsible for authorising operations in which they are directly involved unless it is unavoidable)

Officers must record on the Authorisation, Review and Renewal Forms the date on which the authorisation should next be reviewed.

#### 14. **Judicial Approval**

- (a) Once an application for the use of **d**Directed **s**Surveillance or for the use or conduct of a CHIS has been authorised by the Authorising Officer, the authorisation then needs to receive judicial approval from a **m**Magistrate (**J**ustice of the **P**ea**c**e).
- (b) The Applicant will need to contact the magistrates' court to arrange an appointment for the application to be made. The Applicant will complete the Judicial Approval **a**Application **f**Form (Form JA1) and prepare a Judicial Approval Order **f**Form (Form JA2) for signature by the Justice of the Peace (JP) The **a**Application **f**Form will contain a brief summary of the circumstances of the case.
- (c) The officer will provide the JP with a copy of the original RIPA authorisation and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. The original RIPA authorisation should be shown to the JP but it will be retained by the local authority. The court may wish to take a copy. The partially completed **j**Judicial **a**Application and **e**Order **f**Forms will be provided to the JP.
- (d) The hearing will be in private and will be heard by a single JP. The JP will read and consider the RIPA authorisation and the **j**Judicial **a**Application and **e**Order **f**Forms. He or she may ask questions to clarify points or to require additional reassurance on particular matters.
- (e) The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for **d**Directed **s**Surveillance has been met.

The **f**Forms and supporting papers must by themselves make the case. It is not sufficient for the officer to provide oral evidence where this is not reflected or supported in the papers provided. The JP may note on the **f**Form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.

- (f) If more information is required to determine whether the authorisation has met the tests then the JP will refuse the authorisation. If an application is refused the local authority should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.
- (g) The JP will record his/her decision on the Judicial Order **f**Form. This will be the official record of the JP's decision. Court staff will retain a copy of the

RIPA authorisation and the **j**udicial **a**pplication and **e**Order **f**orms. This information will be retained securely.

(h) The decisions that the JP can make are as follows:

1. Approve the grant or renewal of the authorisation;
2. Refuse to approve the grant or renewal of an authorisation;
3. Refuse to approve the grant or renewal and quash the authorization.

If the JP refuses to grant or renew the authorisation it will not take effect and the local authority may not use the technique in that case.

- (i) The authorisation will be granted at the time that it is approved by the JP. If it is not renewed, the authorisation will cease to have effect at the end of a period of three months (for Directed Surveillance) or 12 months (for the use of a CHIS) starting with the time it was approved by the JP. It is important that the expiry date is correctly recorded by using the date of judicial approval, rather than the date of approval by the Authorising Officer.
- (j) Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the **f**orm may be remedied without the Council going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken. If the JP decides to quash the original authorisation, the court must not exercise its power to quash that authorisation unless the Applicant has had at least 2 business days from the date of the refusal in which to make representations. [There is still a requirement to record and file, in the Central Register, applications which are refused.](#)
- (k) The Council will need to obtain judicial approval for all initial RIPA authorisations/applications as well as for all renewals and officers will need to retain a copy of the **j**udicial **a**pplication and **e**Order **f**orms after they have been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.
- (l) On rare occasions officers might have need for out of hour's access to a JP so the officer will need to make the necessary arrangements with the court staff. The officer will need to provide two partially completed **j**udicial **a**pplication and **e**Order **f**orms so that one can be retained by the JP. The officer should provide the court with a copy of the signed judicial application and order forms on the next working day.
- (m) Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the investigating officer's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.
- (n) If the magistrates make any pertinent comments to the Applicant about the quality of the application or the information contained in it, the Applicant should promptly report this back to the Authorising Officer. This is so that any necessary action can be taken to incorporate or address these issues. It

would be best practice for the Authorising Officer to make a record of any such comments and any action that is taken.

~~(e) The introduction of these additional rules means that the Council is not able to orally authorise the use of RIPA techniques.~~

### **Additional Safeguards when Authorising a CHIS**

15. When authorising the conduct or use of a CHIS, the Authorising Officer must also:-
- (a) be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved;
  - (b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;
  - (c) consider the likely degree of intrusion of all those potentially affected;
  - (d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained;
  - (e) ensure records containing particulars are not available except on a need to know basis; and
  - (f) consider the ongoing security and welfare of the CHIS after the authorisation is cancelled.

### **16. Urgent Authorisations**

~~Because of the need for judicial approval of all authorisations it is no longer possible for the Council will be able to make use of oral authorisations in urgent cases.~~

### **167. Duration**

- (a) The Form must be reviewed in the time stated and cancelled once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from approval of the authorisation by a Justice of the Peace) for Directed Surveillance, and for 12 months (from approval of the authorisation by a Justice of the Peace) for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, the Forms do not expire! The ~~f~~Forms have to be reviewed and/or cancelled (once they are no longer required)!
- (b) Authorisations cannot be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.
- (c) The renewal will begin on the day when the authorisation would have expired.

## U. Working With / Through Other Agencies

1. When an individual or non-governmental organisation is acting under the direction of the Council then they are acting as the agent of the Council. Any activities that they conduct that meet the definition of ~~d~~Directed ~~s~~Surveillance should be considered for authorisation under RIPA. Consequently, when some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this Document and the Forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.
2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue, and Department of Work & Pensions etc):-
  - (a) wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to ~~allow the Council's resources to be used for the other agency's purposes~~ ~~such use~~, s/he must obtain a copy of that agency's RIPA ~~authorisation form for the record~~ (a copy of which must be ~~passed to the Service Director for~~ ~~maintained with~~ the Central Register) and/or relevant extracts from the same or a letter from the agency confirming the existence of the RIPA authorisation which are sufficient for the purposes of protecting the ~~County Borough~~ Council and the use of its resources;
  - (b) wishes to use the Council's premises for their own RIPA action, the Officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be ~~so used for the agency's activities~~. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA ~~f~~Forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.
3. In terms of 2(a), if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.
4. Where it is foreseen that the operational support of another agency, such as the police, will be involved in carrying out the surveillance then this involvement should be explicitly stated on the authorisation. There is no need for the other agency to obtain a separate authorisation. Officers must ensure that officers from the other agency are made aware of the extent and limitations of the authorisation.

5. In cases where the authorisation for the use of a CHIS will benefit agencies in addition to the Council, the responsibility for the management of the CHIS may be taken up by one of the agencies on behalf of the others.
6. -If in doubt, please consult with the Senior Responsible Officer at the earliest opportunity.

#### **JK. Record Management**

1. The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in Divisions and a Central Register of all Authorisation Forms will be maintained and monitored by the Senior Responsible Officer. These records should be kept for at least 3 years from the ending of each authorisation, ~~although it would be best practice to retain these records for 5 years.~~

#### **Records maintained in the Division**

- ~~2. The following documents must be retained by the relevant Chief Officer (or his/her Divisional Co-ordinator) for such purposes:
  - a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
  - a record of the period over which the surveillance has taken place;
  - the frequency of reviews prescribed by the Authorising Officer;
  - a record of the result of each review of the authorisation;
  - a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
  - the date and time when any instructions regarding cancellations or urgent approvals were given by the Authorising Officer;
  - the Unique Reference Number for the authorisation.~~
- ~~3. Each form will have a unique reference number. The cross-referencing of each reference number takes place within the Forms for audit purposes. Rejected Forms will also have reference numbers.~~
- ~~4. The only records that need to be maintained centrally for the use of a CHIS are the name or code name of the CHIS, the dates of authorisation, renewal and cancellation of an authorisation and whether the activities were self authorised. Copies of the CHIS 4 form and any risk assessment should be retained by the Council but these do not need to be retained on the central register.~~

## Central Register maintained by the Senior Responsible Officer

52. Authorising Officers must forward the original ~~a~~A~~u~~thorising ~~f~~F~~o~~r~~m~~ (and any review / renewal / cancellation and rejection of the same) plus a copy of any ~~j~~J~~u~~dicial ~~a~~A~~p~~proval ~~e~~O~~r~~der ~~f~~F~~o~~r~~m~~ as soon as is practicable. The Senior Responsible Officer will monitor the same and give appropriate guidance, from time to time, or amend this Document, as necessary

63. The Central Record ~~for directed surveillance~~ will consist of:

- Date and time of authorisation
- Name & grade of Authorising Officer
- A Unique Reference Number for the investigation
- Title of operation including the names of the subjects if known
- ~~Whether urgency provisions used~~
- Details of attendances at the ~~m~~M~~a~~gistrates' ~~e~~C~~o~~urt for judicial approval, (This will consist of the date of attendance at court, the determining magistrate, the decision of the court and the time and date of that decision)
- Dates of any reviews
- Date of renewal
- Name and grade of Authorising Officer granting renewal
- Whether investigation is likely to result in obtaining confidential material
- Whether Authorising Officer was directly involved in the investigation
- Date of cancellation
- Name / Code name of CHIS
- Individual CHIS risk assessment

74. Council will retain records for a period of at least three years from the ending of the authorisation. The ~~Office of the Surveillance Commissioners (OSC)~~Investigatory Powers Commissioner's Office (IPCO) can audit/review the Council's policies and procedures, and individual authorisations.

### 85. Gatekeeper Role

As a number of different Authorising Officers are entitled to authorise the use of ~~e~~D~~i~~rected ~~s~~S~~u~~rveillance or the use of a CHIS it is important that the quality of all such authorisations is checked for consistency by or on behalf of the Senior Responsible Officer.

On receipt of the authorisation the Secretary to the Senior Responsible Officer will check the central register to ascertain whether or not another officer is authorised to undertake such activities at that address or in that area and, if this occurs, will bring this overlap to the attention of the proposed Authorising Officer.

The Senior Responsible Officer or a solicitor acting on his behalf will examine in detail all the authorisations when they are received at the central register. If any such authorisation is found not to meet the high standards expected in Rhondda Cynon Taff the solicitor, on behalf of the Senior Responsible Officer, will instruct the Authorising Officer to immediately cancel the authorisation. If the difficulties can be overcome, a new application must be made by the



Applicant and carefully assessed by the Authorising Officer, bearing in mind the concerns of the Senior Responsible Officer. If it is decided that the granting of an authorisation for this investigation will not be appropriate, for reasons of lack of necessity or proportionality or otherwise, the Applicant will be instructed that no surveillance may be used in this investigation.

### Use of CCTV Cameras

~~96. Copies of all authorisations in respect of the use of Council owned CCTV cameras must be sent to the CCTV control room.~~

### KL. Oversight of exercising of functions

#### 1. Senior Responsible Officer

The Senior Responsible Officer is responsible for:

- Ensuring that all Authorising Officers are of an appropriate standard
- The integrity of the processes of authorising surveillance and the management of the use of a CHIS;
- Compliance with the act and codes of practice;
- Oversight of the reporting of errors to the ~~Office of Surveillance Commissioners (OSC)~~Investigatory Powers Commissioner's Office (IPCO), identification of causes of errors and implementation of processes to minimise repetition of errors
- Engaging with ~~OSC~~IPCO inspectors when they conduct inspections;
- Overseeing the implementation of any post-inspection action plans recommended by the ~~OSC~~IPCO;

The Director of Legal and Democratic Services is the Senior Responsible Officer with regard to the use of ~~d~~Directed ~~s~~Surveillance or the use of a CHIS.

The ~~Office of Surveillance Commissioners~~IPCO allows only the SRO to make requests for guidance from them.

#### 2. Elected Members

- Every year elected members should review the Council's use of RIPA and set the Corporate Policy for the use of RIPA.
- On a regular basis elected members should consider an internal report from the Senior Responsible Officer to ensure that the use of RIPA is consistent with Corporate Policy and that the Corporate Policy remains fit for its purpose.
- Elected members should not be involved in making decisions on specific authorisations.

#### 3. Office of Surveillance CommissionersInvestigatory Powers Commissioner's Office

The ~~Office of Surveillance Commissioners~~IPCO regularly carries out inspections to review how the Council makes use of RIPA. The Commissioners then produce a report on the inspection of how the Council

exercises and performs its powers under the legislation. The reports may make recommendations to help the Council improve and implement good practice. The Senior Responsible Officer will ensure that a post inspection plan is made to implement these recommendations and that the improvements are then introduced.

The OSC-IPCO advises that, if views about a particular issue are received from the OSC-IPCO inspector during the inspection, it would be unwise for officers to extrapolate guidance provided in one context to all other situations.

#### 4. **Investigatory Powers Tribunal**

The Investigatory Powers Tribunal has been introduced by the legislation and it is made up of senior members of the judiciary and the legal profession. It is independent of the government. The Tribunal has full powers to investigate and decide on any cases within its jurisdiction that are referred to it.

#### **LM. Concluding Remarks**

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this Document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.
2. Obtaining an authorisation under RIPA and following this Document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.
3. Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must never sign ~~or rubber stamp~~ Form(s) without thinking about their personal and the Council's responsibilities.
4. Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the ~~f~~Form and the ~~f~~Form retained for future audits.
5. For further advice and assistance on RIPA, please contact the Senior Responsible Officer. Details are as follows:-

Paul J LucasChristopher B Jones,  
Director Legal and Democratic Services  
The Pavilions,  
Cambrian Park,  
Tonypany.  
CF40 2XX

Tel: (01443) 424105

Fax: ~~(01443) 424114~~

E-mail: [paul.j.lucaschris.b.jones@rhondda-cynon-taffrctcbc.gov.uk](mailto:paul.j.lucaschris.b.jones@rhondda-cynon-taffrctcbc.gov.uk)

DRAFT

## APPENDIX 1

### List of Authorising Officer Posts

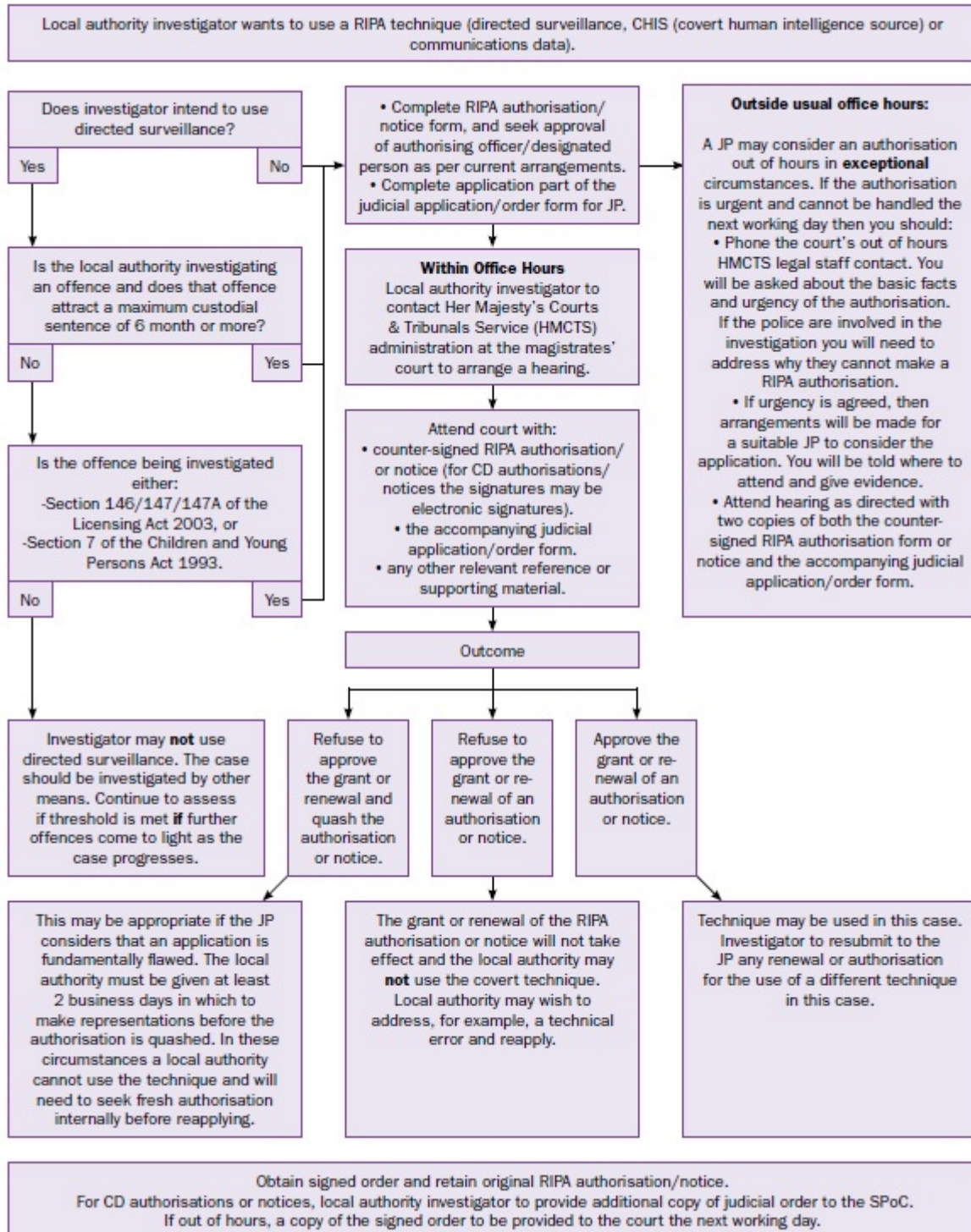
GROUP	Name of Contact Officer
<p><b>CHIEF EXECUTIVE</b>  <i>Authorising Officers:</i>            Chief Executive  <u>Director of Legal and Democratic Services</u>  <u>Head of Legal – Litigation, Planning &amp; Environment and Community and Children’s Services</u>  <del>Director of Regeneration and Planning</del>  <u>Service Director, Planning</u></p>	<ul style="list-style-type: none"> <li>- Chris Bradshaw</li> <li>- <u>Chris Jones</u></li> <li>- <u>Paul Nicholls</u></li> <li>- <del>Jane Cook</del></li> <li>- <u>Simon Gale</u></li> </ul>
<p><b>CORPORATE <u>AND FRONTLINE</u> SERVICES</b>  <i>Authorising Officers:</i>  <u>Director of Highways and Streetcare Services</u>  <u>Head of Streetcare Services</u>  <u>Head of Revenues and Benefits</u>  <del>Director of Legal and Democratic Services</del>  <del>Service Director, Legal and Democratic Services</del>  <del>Principal Solicitor</del>  <del>Solicitor</del>  <del>Head of Reviews and Benefits</del>  <del>Team Manager Benefits</del></p>	<ul style="list-style-type: none"> <li>- <u>Nigel Wheeler</u></li> <li>- <u>Steve Owen</u></li> <li>- <u>Matthew Phillips</u></li> <li><u>Paul Lucas</u></li> <li>- <del>Chris Jones</del></li> <li>- <del>Paul Nicholls</del></li> <li>- <del>Simon Humphreys</del></li> <li>- <del>Andrew Symes</del></li> <li>- <del>Helen Phillips</del></li> </ul>
<p><b>COMMUNITY &amp; CHILDREN’S SERVICES</b>  <i>Authorising Officers:</i>  <del>Service Director, - Public Health, &amp; Protection and Community Services</del>  <del>Environmental Head of Public Protection Manager</del>  <del>Community Safety Manager</del>  <del>Trading Standards Manager</del>  <del>Housing and Enforcement Project Strategy and Investment Manager</del>  <del>Food and Health and Safety Manager</del>  <del>Pollution and Public Health Manager</del>  <del>Licensing Manager</del></p>	<ul style="list-style-type: none"> <li>- Paul Mee</li> <li>- Louise Davies</li> <li>- <u>Andrew Mallin</u></li> <li>- <u>Judith Parry</u> <del>Tony</del></li> <li><u>O’Leary</u></li> <li>- Jennifer Ellis</li> <li>- <u>Amy Lewis</u></li> <li>- Neil Piliner</li> <li>- <u>Meryl Williams</u></li> </ul>
<p><del>Service Director Planning</del>  <del>Manager Special Projects</del>  <del>Planning Enforcement Manager</del></p> <p><del>Service Director for Highways &amp; Streetcare</del>  <del>Head of Streetcare</del></p>	<ul style="list-style-type: none"> <li>- <del>Simon Gale</del></li> <li>- <del>Jim Bailey</del></li> <li>- <del>Julie Williams</del></li> <li>- <del>Nigel Wheeler</del></li> <li>- <del>Steve Owen</del></li> </ul>

## IMPORTANT NOTES

- A. All persons employed in the posts identified above must receive appropriate training.
- B. Only the ~~Head of Paid Service~~Chief Executive is authorised to sign Forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph **G** of this Document).
- C. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Senior Responsible Officer for consideration, as necessary.
- D. If in doubt, ask the Senior Responsible Officer BEFORE any ~~e~~Directed ~~s~~Surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

DRAFT

RIPA FLOW CHART



NB: If in doubt, ask the Senior Responsible Officer BEFORE any **d**irected **s**urveillance and/or CHIS is authorised, renewed, cancelled, or rejected. Chief Officers will designate members of their staff to be a Divisional. Co-ordinators for the purpose of RIPA and advise the Senior Responsible Officer accordingly.

## APPENDIX 3

### Specific Examples from RIPA Code of Practice

#### Directed Surveillance Code of Practice

##### Private information

###### **Example 1**

Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A ~~e~~Directed ~~s~~Surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation.

###### **Example 2**

Officers of a local authority wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a ~~e~~Directed ~~s~~Surveillance authorisation, as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a ~~e~~Directed ~~s~~Surveillance authorisation should be considered.

###### **Example 3**

A surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A ~~e~~Directed ~~s~~Surveillance authorisation should therefore be sought.

##### Intrusive surveillance

###### **Example 1**

~~An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, the use of a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.~~

##### Immediate response

###### **Example 1**

An authorisation under the 2000 Act would not be appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol.

## **General observation duties**

### ***Example 1***

Plain clothes police officers on patrol to monitor a high street crime hot-spot or prevent and detect shoplifting would not require a **d**Directed **s**Surveillance authorisation. Their objective is merely to observe a location and, through reactive policing, to identify and arrest offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance of individuals, and the obtaining of private information is unlikely. A **d**Directed **s**Surveillance authorisation need not be sought.

### ***Example 2***

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

### ***Example 3***

Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A trained employee or person engaged by a public authority is deployed to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the Act, that a public authority may conclude that a covert human intelligence source (CHIS) authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation.

### ***Example 4***

Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine her suspected involvement in shoplifting. It is proposed to conduct covert surveillance of Z and record her activities as part of the investigation. In this case, private life considerations are likely to arise where there is an expectation of privacy and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. A **d**Directed **s**Surveillance authorisation should be considered.

## **Not relating to core functions**

### ***Example 1***

A police officer is suspected by his employer of undertaking additional employment in breach of discipline regulations. The police force of which he is a member wishes to conduct covert surveillance of the officer outside the police work environment. Such activity, even if it is likely to result in the obtaining of private information, does not constitute **d**Directed **s**Surveillance for the purposes of the 2000 Act as it does not relate to the discharge of the police force's core functions. It relates instead to the carrying out of ordinary functions, such as employment, which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and employment practices code.

### ***Example 2***



~~A police officer claiming compensation for injuries allegedly sustained at work is suspected by his employer of fraudulently exaggerating the nature of those injuries. The police force of which he is a member wishes to conduct covert surveillance of the officer outside the work environment. Such activity may relate to the discharge of the police force's core functions as the police force may launch a criminal investigation. The proposed surveillance is likely to result in the obtaining of private information and, as the alleged misconduct amounts to the criminal offence of fraud, a directed surveillance authorisation may be appropriate.~~

## **CCTV and ANPR**

### ***Example 1***

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

### ***Example 2***

A local police team receives information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be considered for authorisation as ~~d~~Directed ~~s~~Surveillance.

## **Proportionality**

### ***Example 1***

An individual is suspected of carrying out a series of criminal damage offences at a local shop, after a dispute with the owner. It is suggested that a period of ~~d~~Directed ~~s~~Surveillance should be conducted against him to record his movements and activities for the purposes of preventing or detecting crime. Although these are legitimate grounds on which ~~d~~Directed ~~s~~Surveillance may be conducted, it is unlikely that the resulting interference with privacy will be proportionate in the circumstances of the particular case. In particular, the obtaining of private information on the individual's daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed.

## **Collateral Intrusion**

### ***Example 1***

HMRC seeks to conduct ~~d~~Directed ~~s~~Surveillance against T on the grounds that this is necessary and proportionate for the collection of a tax. It is assessed that such surveillance will unavoidably result in the obtaining of some information about members of T's family, who are not the intended subjects of the surveillance. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the

authorisation. This may include not recording or retaining any material obtained through such collateral intrusion.

### **Example 2**

A law enforcement agency seeks to conduct a covert surveillance operation to establish the whereabouts of N in the interests of preventing a serious crime. It is proposed to conduct **eDirected sSurveillance** against P, who is an associate of N but who is not assessed to be involved in the crime, in order to establish the location of N. In this situation, P will be the subject of the **eDirected sSurveillance** authorisation and the authorising officer should consider the necessity and proportionality of conducting **eDirected sSurveillance** against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that **eDirected sSurveillance** of P will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the authorising officer.

## **Online Covert Activity (1) – Directed Surveillance**

### **Example 1**

A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

### **Example 2**

A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

### **Example 3**

A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

## **Online Covert Activity (2) – CHIS**

### **Example 1**

An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.

### **Example 2**

HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

### **Example 3**

An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.

### **Example 4**

The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A Directed Surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.

## **Updating authorisations by review**

### ***Example 1***

A **d**Directed **s**Surveillance authorisation is obtained by the police to authorise surveillance of “X and his associates” for the purposes of investigating their suspected involvement in a crime. X is seen meeting with A in a café and it is assessed that subsequent surveillance of A will assist the investigation. Surveillance of A may continue (he is an associate of X) but the **d**Directed **s**Surveillance authorisation should be amended at a review to include “X and his associates, including A”.

## **Covert Human Intelligence Source Code of Practice**

### **Establishing, maintaining and using a relationship**

#### ***Example 1***

Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a **d**Directed **s**Surveillance authorisation.

#### ***Example 2***

In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing he has first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain his trust, in order to

purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.

### **Public Volunteers**

#### ***Example 1***

A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.

#### ***Example 2***

A caller to a confidential hotline (such as Crimestoppers, the Customs Hotline, the Anti-Terrorist Hotline, or the Security Service Public Telephone Number) reveals that he knows of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information, an authorisation for the use or conduct of a CHIS may be appropriate

### **Tasking not involving a relationship**

#### ***Example 1***

A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, **Directed Surveillance** may need to be considered where there is an interference with the Art 8 rights of an individual

### **Identifying when a human source becomes a CHIS**

#### ***Example 1***

Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private and family life of Mr Y's work colleague.

### **Collateral intrusion**

#### ***Example 1***

An undercover operative is deployed to obtain information about the activities of a suspected criminal gang under CHIS authorisation. It is assessed that the operative

will in the course of this deployment obtain private information about some individuals who are not involved in criminal activities and are of no interest to the investigation. The authorising officer should consider the proportionality of this collateral intrusion, and whether sufficient measures are to be taken to limit it, when granting the authorisation.

### **Example 2**

The police seek to establish the whereabouts of Mr W in the interests of national security. In order to do so, an undercover operative is deployed to seek to obtain this information from Mr P, an associate of Mr W who is not of direct security interest. An application for a CHIS authorisation is made to authorise the deployment. The authorising officer will need to consider the necessity and proportionality of the operation against Mr P and Mr W, who will be the direct subjects of the intrusion. The authorising officer will also need to consider the proportionality of any collateral intrusion that will arise if there is any additional interference with the private and family life of other individuals of no interest to the investigation.

## **Reviewing and renewing authorisations**

### **Example 1**

An authorisation is obtained by the police to authorise a CHIS to use her relationship with “Mr X and his close associates” for the covert purpose of providing information relating to their suspected involvement in a crime. Mr X introduces the CHIS to Mr A, a close associate of Mr X. It is assessed that obtaining more information on Mr A will assist the investigation. The CHIS may use her relationship with Mr A to obtain such information but the review of the authorisation should specify any interference with the private and family life of “Mr X and his associates, including Mr A” and that such an interference is in accordance with the original authorisation

## **Specific situations not requiring authorisation**

### **Noise Nuisance**

~~The covert recording of suspected noise nuisance where: the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm) or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be required.~~

### **Recording of interviews**

~~The recording, whether overt or covert, of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a member of a public authority. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a member of a public authority and that information gleaned through the interview has passed into the possession of the public authority in question.~~

## APPENDIX 4

### RIPA DS FORMS : DIRECTED SURVEILLANCE

Form DS 1 : Application for authorisation to carry out **eD**irected **sS**urveillance.

Form DS 2 : Application for Renewal of Form DS 1.

Form DS 3 : Review of Form DS 1.

Form DS 4 : Cancellation of Form DS 1.

**NB: If in doubt, ask the Senior Responsible Officer BEFORE any **eD**irected **sS**urveillance and/or CHIS is authorised, renewed, cancelled or rejected.**

DRAFT

<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

**PART II OF THE REGULATION OF INVESTIGATORY  
POWERS ACT (RIPA) 2000**

**APPLICATION FOR AUTHORISATION TO CARRY OUT  
DIRECTED SURVEILLANCE**

<b>Public Authority  (Including full address)</b>			
<b><u>Name of Applicant</u></b>		<b><u>Unit/Branch/Division</u></b>	
<b><u>Full Address</u></b>			
<b>Contact Details</b>			
<b>Investigation/Operation Name (if applicable)</b>			
<b>Investigating Officer (if a person other than the applicant)</b>			

**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.<sup>1</sup>**

--

<sup>1</sup>For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

**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:



<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

**5. Explain the information that it is desired to obtain as a result of the directed surveillance. Please include how the information will assist the investigation.**

**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. (SI 2012 No.1500)***

For the purpose of preventing or detecting conduct which:-  
 Constitutes one or more criminal offences, namely .....

AND

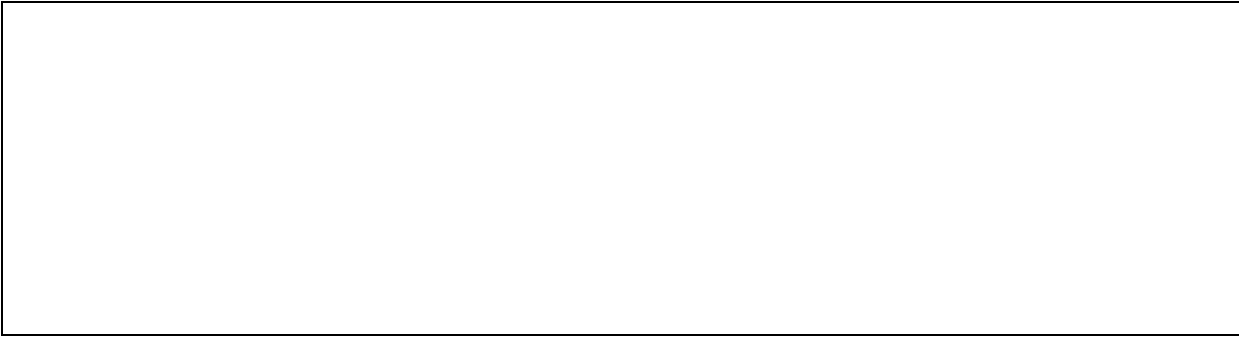
At least one of the criminal offences is punishable, whether on summary conviction or on indictment, by a maximum term of imprisonment of at least 6 months of imprisonment, namely .....

OR

Is an offence under Section 146, 147 or 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933 or Section 91 or 92 of the Children and Families Act 2014

**Background information about these types of offences and the kind of evidence that is needed to prove the offences is provided as a separate document (Optional)**

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



DRAFT

Directed Surveillance Unique Reference Number (URN)	
---	--

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs [3-84.11](#) to [3-114.19](#)]

*Describe precautions you will take to minimise collateral intrusion*

Blank response area for question 8.

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 [34.4](#) to [3-74.10](#)]

Blank response area for question 9.

Directed Surveillance Unique Reference Number (URN)	
---	--

**10. Confidential information. [Code paragraphs 4-19.23 to 4-319.72]**

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

**11. Applicant's Details**

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

**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?*]

Directed Surveillance Unique Reference	
---	--

Number (URN)	
--------------	--

13. Explain why you believe the directed surveillance is necessary. [Code paragraph [3.34.5](#)]

Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraphs [3.44.6](#) to [3.74.9](#)]

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs [4.19.23](#) to [4.319.72](#)

Date of first review	
----------------------	--

Directed Surveillance Unique Reference Number (URN)	
---	--

Programme for subsequent reviews of this authorisation: [Code paragraph [3.234.34 to 4.39](#)]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

<b>Name (Print)</b>		<b>Grade/Rank</b>	
<b>Signature</b>		<b>Date and time</b>	
<b>Justice of the Peace granting Judicial Approval</b>		<b>Date and time of judicial approval</b>	
<b>Expiry date and time [e.g.: authorisation granted on 1 April 2005 – expires on 30 June 2005, 23:59]</b>			

**15. Is Authorising officer directly involved in this Investigation/Operation?**

YES/NO

<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

~~16. Urgent Authorisation [Code paragraphs 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.~~

~~17. 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~~

<b>Name (Print)</b>		<b>Grade/Rank</b>		
<b>Signature</b>		<b>Date and Time</b>		
<b>Urgent authorisation Expiry date:</b>		<b>Expiry time:</b>		
<i>Remember the 72 hour rule for urgent authorities – check Code of Practice</i>	e.g. authorisation granted at 5pm on June 1 <sup>st</sup> expires 4:59pm on 4 <sup>th</sup> June			

Directed Surveillance Unique Reference Number (URN)	
---	--

**PART II OF THE REGULATION OF INVESTIGATORY  
POWERS ACT (RIPA) 2000**

**APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE  
AUTHORISATION**

(Please attach the original authorisation)

<b>Public Authority</b> <i>(including full address)</i>			
<b>Name of Applicant</b>		<b>Unit/Branch/ Division</b>	
<b>Full Address</b>			
<b>Contact Details</b>			
<b>Investigation/Operation Name (if applicable)</b>			
<b>Renewal Number</b>			

**Details of Renewal:**

<b>1. Renewal numbers and dates of any previous renewals.</b>	
<b>Renewal Number</b>	<b>Date</b>



<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

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

--

**4. Detail 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.**

--

<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

<b>7. Applicants Details</b>			
<b>Name (Print)</b>		<b>Tel. No.</b>	
<b>Grade/Rank</b>		<b>Date</b>	
<b>Signature</b>			

<b>8. Authorising Officer's Comments. <u>This box must be completed.</u></b>

<b>9. Authorising Officer's Statement.</b>				
<p>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.</p> <p>This authorisation will be reviewed frequently to assess the need for the authorisation to continue.</p>				
Name (Print) .....		Grade/Rank.....		
Signature .....		Date .....		
<b>Renewal From:</b>	<b>Time:</b>	<b>Date:</b>		
<b>Name of Justice of the Peace granting Judicial Approval</b>				
<b>Signature</b>		<b>Date and time of judicial approval</b>		
<b>Expiry date and time [e.g.: authorisation granted on 1 April 2005 – expires on 30 June 2005, 23:59]</b>				

<b>Date of first review.</b>	
------------------------------	--

Date of subsequent reviews of this authorisation.	
---	--

DRAFT

Directed Surveillance Unique Reference Number (URN)	
---	--

**PART II OF THE REGULATION OF INVESTIGATORY  
POWERS ACT (RIPA) 2000**

**REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION**

<b>Public Authority</b> <i>(including full address)</i>			
<b>Applicant</b>		<b>Unit/Branch/ Division</b>	
<b>Full Address</b>			
<b>Contact Details</b>			
<b>Operation Name</b>		<b>Operation Number* *Filing Ref</b>	
<b>Date of Authorisation or Last Renewal</b>		<b>Expiry Date of Authorisation or Last Renewal</b>	
		<b>Review Number</b>	

**Details of Review:**

<b>1. Review number and dates of any previous reviews.</b>	
<b>Review Number</b>	<b>Date</b>

<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

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

**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 occurring.**

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

<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

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

<b>8. Review Officer's comments, including whether or not the directed surveillance should continue.</b>

<b>9. Authorising Officer's Statement.</b>
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].
<b>Name (Print)</b> ..... <b>Grade/Rank</b> ..... <b>Signature</b> ..... <b>Date</b> .....

<b>10. Date of next review.</b>	
---------------------------------	--

Directed Surveillance Unique Reference Number (URN)	
---	--

**PART II OF THE REGULATION OF INVESTIGATORY  
POWERS ACT (RIPA) 2000**

**CANCELLATION OF A DIRECTED  
SURVEILLANCE AUTHORISATION**

<b>Public Authority</b> <i>(including full address)</i>			
<b>Name of Applicant</b>		<b>Unit/Branch/ Division</b>	
<b>Full Address</b>			
<b>Contact Details</b>			
<b>Investigation/Operation Name (if applicable)</b>			

**Details of cancellation:**

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

--

<b>Directed Surveillance Unique Reference Number (URN)</b>	
--	--

<b>2. Explain the value of surveillance in the operation:</b>

<b>3. Explain the outcome that was obtained from using the surveillance:</b>

<b>4. Identify a) the types of products of surveillance that were obtained in the operation and b) how they will be securely stored or disposed of:</b>

<b>5. Authorising officer's statement.</b>
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.
<b>Name (Print)</b> ..... <b>Grade</b> .....
<b>Signature</b> ..... <b>Date</b> .....

<b>6. Time and Date of when the authorising officer instructed the surveillance to cease.</b>			
<b>Date:</b>		<b>Time:</b>	

<b>7. Authorisation cancelled.</b>	<b>Date:</b>	<b>Time:</b>



**APPENDIX 5.**

**RIPA B FORMS : COVERT HUMAN INTELLIGENCE SOURCE (CHIS)**

**Form CHIS 1** : Application for authorisation of the Use or Conduct of a Covert Human Intelligence Source (CHIS).

**Form CHIS 2** : Application for Renewal of Form CHIS 1.

**Form CHIS 3** : Cancellation of Form CHIS 1.

**Form CHIS 4** : Record of Use

**Form CHIS 5** : Review of Form CHIS 1.

**NB: If in doubt, ask the Senior Responsible Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.**

DRAFT

CHIS Unique Reference Number (URN)	
------------------------------------	--

**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)**

<b>Public Authority</b> <i>(including full address)</i>			
<b>Name of Applicant</b>		<b>Service/Department/ Branch</b>	
How will the source be referred to? i.e. what will be his/her pseudonym or reference number			
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)			
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)?			
<b>Investigation/Operation Name (if applicable)</b>			

**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<sup>1</sup>.**

--

<b>CHIS Unique Reference Number (URN)</b>	
---	--

**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. Please explain how achieving this purpose will assist the investigation.**

--

**4. Describe in detail the proposed covert conduct of the source or how the source is to be used**

--

<sup>1</sup> For Local Authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards rather than officer responsible for the management of an investigation.

5. Identify on which grounds the conduct or the use of a source is necessary under Section 29(3) of RIPA. *Delete those that are in applicable. Ensure that you know which of these grounds you are entitled to rely on. (SI 2010 No. 521)*

- For the purpose of preventing or detecting crime or of preventing disorder;

Background information about these types of offences and the kind of evidence that is needed to prove the offences is provided as a separate document (Optional)

CHIS Unique Reference Number (URN)	
------------------------------------	--

6. Explain why this conduct or use of a source is necessary on the grounds you have identified [Code paragraph 3.2 to 3.3]

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8-9 to 3.11-12]

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 3.17-18 to 3.198)?

9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.413 to 6.15).

10. Explain why this conduct or use of a source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? And why is this intrusion outweighed by the need for a source in operational terms or can the evidence be obtained by any other means? [Code paragraphs 3.3-4 to 3.5]

<b>CHIS Unique Reference Number (URN)</b>	
---	--

**11. Confidential information [Code paragraph 4.18.26 to 4.218.71]**  
**Indicate the likelihood of acquiring any confidential information**

**12. Applicant's Details**

<b>Name (Print)</b>		<b>Grade/Rank/ Position</b>	
<b>Signature</b>		<b>Tel No:</b>	
<b>Date</b>			

**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 identify the pseudonym or reference number of the source, not the true identity**

I hereby authorise the conduct or the use of a covert human intelligence source defined as follows: *[Why is the conduct or use of the source necessary, with Whom will the source establish or maintain a relationship for a covert purpose or to covertly use the relationship, What conduct is being authorised, Where and When will the source undertake the conduct authorised, How will the source undertake the conduct authorised?]*

**This authorisation will cease to have effect at the end of a period of 12 months unless renewed. The authorisation will be reviewed frequently to assess the need for the authorisation to continue.**

14. Explain why you believe the conduct or use of the source is necessary. [Code paragraph 3.2 to 3.3]

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 3.34 to 3.5]

15 (Confidential Information Authorisation). Supply detail demonstrating compliance with Code paragraphs 8.264.1 to 4.218.71

16. Date of first review:

**17. Programme for subsequent reviews of this authorisation: [Code paragraphs 5.153.13 and 5.163.17]. 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**

<b>Name (Print)</b>		<b>Grade/Rank/Position</b>	
<b>Signature</b>		<b>Time and date granted</b> <b>Time and date authorisation ends</b>	
<b>Justice of the Peace granting judicial approval</b>		<b>Time and date of judicial approval</b>	

*Remember an authorisation may be granted for a 12 month period, ie 17:00 hrs 4 June 2006 to 2359 hrs 3 June 2007*

**19. Is Authorising officer directly involved in this Investigation/Operation?**

<u>YES/NO</u>
---------------

**20. 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.**

--



<b>CHIS Unique Reference Number (URN)</b>	
---	--

~~21. 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.~~

~~22. Authorising Officer of urgent authorisation~~

<b>Name (Print)</b>		<b>Grade/Rank/ Position</b>	
<b>Signature</b>		<b>Date and Time</b>	
<b>Urgent authorisation Expiry date:</b>		<b>Expiry time:</b>	

~~Remember the 72 hour rule for urgent authorities — check Code of Practice [Code Paragraph 4.18]. e.g. authorisation granted at 17:00pm on 1<sup>st</sup> June 2006 expires 16:59pm on 4<sup>th</sup> June 2006.~~

CHIS Unique Reference Number (URN)	
---------------------------------------	--

**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)

<b>Public Authority</b> <i>(including full address)</i>	
--	--

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

Details of renewal:

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

<b>CHIS Unique Reference Number (URN)</b>	
---	--

**2. Detail any significant changes to the information in the previous authorisation.**

--

**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.**

--

<b>CHIS Unique Reference Number (URN)</b>	
---	--

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

<b>Name (Print)</b>		<b>Tel. No.</b>	
<b>Grade/Rank</b>		<b>Date</b>	
<b>Signature</b>			

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

--

<b>CHIS Unique Reference Number (URN)</b>	
---	--

**11. Authorising Officer's Statement. The authorisation should identify the pseudonym or reference number of the source not the true identity.**

I, [insert name], hereby authorise the renewal of the conduct/use of the source as detailed above. The renewal of this authorisation will last for 12 months unless further 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:**

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

<b>Name of Justice of the Peace granting Judicial Approval</b>				
<b>Signature</b>		<b>Date and time of judicial approval</b>		
<b>Expiry date and time [e.g.: authorisation granted on 1 April 2005 – expires on 30 June 2005, 23:59]</b>				

<b>Date of first review:</b>	
<b>Date of subsequent reviews of this authorisation:</b>	

<b>Operation Reference Number*</b> (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**

<b>Public Authority</b> <i>(including full address)</i>	
--	--

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

**Details of cancellation:**

<b>1. Explain the reason(s) for the cancellation of the authorisation:</b>

<b>Operation Reference Number*</b> (Filing Ref)	
---	--

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

--

**3. Explain the outcome that was obtained from using the source:**

--

**4. Identify if technical surveillance equipment was used by the source in the operation and, if so, state what information was recorded by the equipment.**

--

**5. Authorising officer's statement. This should identify the pseudonym or reference number of the source not the true identity**

--

<b>Name (print)</b>		<b>Grade:</b>	
<b>Signature</b>		<b>Date</b>	

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

<b>Date:</b>		<b>Time:</b>	
--------------	--	--------------	--

<b>7. Authorisation cancelled.</b>	<b>Date:</b>	<b>Time:</b>

DRAFT



**Record of Use of a Covert Human Intelligence Source**

Identity of the Source.	
Identity or Identities used by the source, where known.	
The means within the authority of referring to the source.	
Any significant information connected with the security and welfare of the source.	
Any risk assessment made in relation to the source.	
Date when and circumstances in which the source was recruited.	

Officer dealing with source on day to day basis	
Officer overseeing use made of source	
Officer maintaining record of use made of source	
Any other authority maintaining records	
Tasks given to the source and the demands made of him in relation to his activities as a source. (i.e. dates and what source was asked to do)	
All contacts or communications between the source and a person acting on behalf of the investigating authority.	
The information obtained by the investigating authority by the conduct or use of the source arising from the above contacts or communications	
The information obtained which is disseminated by the investigating authority.	

CHIS Unique Reference Number (URN)	
------------------------------------	--

**PART II OF THE REGULATION OF INVESTIGATORY  
POWERS ACT (RIPA) 2000**

**REVIEW OF A COVERT HUMAN INTELLIGENCE  
SOURCE (CHIS) AUTHORISATION**

<b>Public Authority</b> <i>(including full address)</i>			
<b>Applicant</b>		<b>Unit/Branch/ Division</b>	
<b>Full Address</b>			
<b>Contact Details</b>			
<b>Operation Name</b>		<b>Operation Number* *Filing Ref</b>	
<b>Date of Authorisation or Last Renewal</b>		<b>Expiry Date of Authorisation or Last Renewal</b>	
		<b>Review Number</b>	

**Details of Review:**

<b>1. Review number and dates of any previous reviews.</b>	
<b>Review Number</b>	<b>Date</b>

<b>CHIS Unique Reference Number (URN)</b>	
---	--

**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 with 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.**

--

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

--

<b>CHIS Unique Reference Number (URN)</b>	
---	--

<b>7. Give details of the review of the risk assessment on the security and welfare of using the source.</b>

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

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

<b>10. Authorising Officer's Statement. The authorisation should identify the pseudonym or reference number of the source not the true identity.</b>	
<b>Name (Print)</b> .....	<b>Grade/Rank</b> .....
<b>Signature</b> .....	<b>Date</b> .....
<b>Date of next review:</b>	

## **CHIS 6**

Risk Assessment of the conduct and use of a source

URN:

### General

The controller must evidence and complete all aspects of the risk assessment personally. Comment on the relationship between handlers and source. For instance do the handlers have the necessary skills to manage the day-to-day requirements of the source? What arrangements are in place for the source to contact the handlers etc? Remember just because your informant's use presents a risk. It does not mean that he or she should not be used. Just analyse, balance, assess and manage their activities.

Risk assessed as: Low/ Medium/ High

### **Council and Community Risks**

Risk assessed as: Low/ Medium/ High

#### Information

#### Source

#### Handler and Controller

#### Council Service Area

#### Public

### **Physical Risks**

Risk assessed as: Low/ Medium/ High

#### Information

#### Source

#### Handlers and controllers

#### Council Service Area

#### Public

### **Psychological Risks**

Risk assessed as: Low/ Medium/ High

#### Source

#### Handlers and controllers

#### Council Service Area

#### Public

### **Legal Risks**

Risk assessed as: Low/ Medium/ High

Information

Source

Handlers and controllers

Council Service Area

Public

**Economic Risks**

Risk assessed as: Low/ Medium/ High

Information

Source

Council Service Area

Public

**Moral Risks**

Risk assessed as: Low/ Medium/ High

Information

Source

Handlers and controllers

Public

Council Service Area

**Management Risks**

Risk assessed as: Low/ Medium/ High

**APPENDIX 6.**

**JUDICIAL APPROVAL FORMS**

**Form JA1:** Judicial Approval Application.

**Form JA2:** Judicial Approval Order Form.

DRAFT



**Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance.  
Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B. FORM JA1**

Local authority: Rhondda Cynon Taff County Borough Council

Local authority department:

Offence under investigation:

Address of premises or identity of subject:

Covert technique requested: (tick one and specify details)

**Communications Data**

**Covert Human Intelligence Source**

**Directed Surveillance**

Summary of details

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

Investigating Officer

Authorising Officer/Designated Person:

Officer(s) appearing before JP:

Address of applicant department:

Contact telephone number:

Contact email address (optional):

Local authority reference:

Number of pages:

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

**FORM JA2**

Magistrates' court:

Having considered the application, I (tick one):

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

Notes:

Reasons:

Signed:

Date:

Time:

Full name:

Address of magistrates' court: