RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

CABINET

30th OCTOBER 2014

REPORT OF THE DIRECTOR OF LEGAL AND DEMOCRATIC SERVICES

Author: Andrew Wilkins, Corporate and Democratic Services Solicitor
Tel No: - (01443) 424189

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) - USE OF RIPA IN 2013-14 BY RHONDDA CYNON TAFF COUNTY BOROUGH COUNCIL

1. PURPOSE

1.1 To enable Members to review the Council's use of the Regulation of Investigatory Powers Act 2000 (RIPA) in 2013 to 2014 and to set the corporate policies for the use of RIPA in 2014 to 2015.

2. RECOMMENDATIONS

2.1 That Members acknowledge that RIPA has been used in an appropriate manner that is consistent with the Council's RIPA policies.

2.2 Adopt a revised corporate RIPA policy (as attached at Appendix 1) to (i) reflect the changes made to the Home Office Codes of Practice and (ii) implement the recommendations arising from the Office of Surveillance Commissioners' inspection

2.3 Adopt a revised corporate policy on the Acquiring of Communications Data (as attached at Appendix 2) following receipt of additional guidance from the Interception of Communications Commissioner's Office.

3. BACKGROUND

3.1 Members are reminded that RIPA provides a statutory mechanism for authorising covert surveillance and the use of a 'covert human intelligence source' (a 'CHIS') (e.g. undercover agents/informants) in circumstances that are likely to result in the obtaining of private information about a person for the purpose of preventing or detecting crime or of preventing disorder. RIPA also controls the acquiring of communications data by Local Authority staff. Its aim is to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action.

3.2 **Use of RIPA in 2013-14 by the Council**

Surveillance and the use of Covert Human Intelligence Resources (CHIS)

3.2.1 During the year from 1st April 2013 to 31st March 2014, 9 new authorisations were granted by Authorising Officers as follows:

- 9 x directed surveillance; and
- 0 x use of a CHIS

The 9 directed surveillance authorisations were issued for the purposes of preventing or detecting conduct which constitutes one or more criminal offences, where at least one of the offences is punishable by a maximum term of imprisonment of at least 6 months (or is under Sections 146, 147 or 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933) in relation to the following:

- 3 x anti-social behaviour;
- 1 x racial abuse at taxi ranks;
- 1 x benefit fraud;
- 1 x sale of illegal tobacco to children;
- 1 x fly tipping;
- 2 x thefts from council property;

3.2.2 At the start of this year the following authorisations that had been authorised in the previous year were carried forward:

- 1 x directed surveillance;
- 0 x use of a CHIS;

The 1 directed surveillance authorisation that had been authorised in the previous year and had been carried forward was also issued for the purposes of preventing or detecting conduct which constitutes one or more criminal offences, where at least one of the offences is punishable by a maximum term of imprisonment of at least 6 months (or is under Sections 146, 147 or 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933) in relation to the following:

- 1 x fly-tipping and theft of fencing;

3.2.3 During the year 10 authorisations for directed surveillance were cancelled and 0 authorisations were carried forward to the following year.

The outcomes of these investigations were as follows:

- 1 x authorisation resulted in 2 persons being identified as having fly-tipped waste. One person was issued with a fixed penalty notice and a prosecution has commenced against the second person;

- 1 x authorisation identified that fly tipping was continuing, but it did not occur in direct view of the cameras so the perpetrators could not be identified;
- 1 x authorisation identified that no significant anti-social behaviour was occurring during the period when the alleged perpetrator was awaiting trial for related issues;
- 1 x authorisation confirmed that the complainant was probably being untruthful in claiming that anti-social behaviour was regularly occurring and that she was probably making these claims because of her mental condition;
- 1 x authorisation showed an incident of criminal damage occurring, but the perpetrator could not be identified due to it taking place in darkness. After this incident the problems stopped. (It is suspected that the perpetrator became aware of the camera in the victim's house);
- 1 x authorisation initially showed that children were buying tobacco at the house, but it did not identify the member of the household who was making the sales. Following one family member leaving the household the sales then completely stopped, so a warning was issued to the householder;
- 1 x authorisation did not identify any racial incidents at the taxi rank, but nevertheless other parts of the same investigation led to 2 persons being prosecuted for racially aggravated offences. The surveillance disproved allegations that the taxi drivers were overcharging and not using their meters;
- 1 x authorisation proved that a man was residing with the benefit claimant and the claimant then cancelled the associated illegal benefit claims;
- 1 x authorisation identified that there might be more that the one person involved with the theft of items from council property, so a more detailed investigation was needed; and
- 1 x authorisation was a follow on to the above theft authorisation and it resulted in a person being arrested by the police and issued with a caution for theft.

3.2.4 The outcomes of some of the cases demonstrate how the use of surveillance is able to produce results that are of clear benefit from an enforcement point of view. In some of the other cases the value of the use of directed surveillance was in establishing that the allegations received by officers were false, or being exaggerated by the provider of the information, or that the problems had stopped because of external causes. Without the use of surveillance officers would not have had any way of finding out whether the allegations were correct or whether the incidents were still continuing. Thus the surveillance has, in effect, prevented unnecessary enforcement action being taken against persons about whom complaints have been received.

3.3 **Communications Data**

3.3.1 During the year from 1st April 2013 to 31st March 2014, 2 applications for communications data were approved.

3.3.2 These applications were issued for the purposes of the prevention and detection of crime or preventing disorder in relation to the following:

- 2 x doorstep crime;

These applications resulted in the obtaining of the following:

Details of the subscriber to 1 telephone number which identified that the telephone number related to an untraceable mobile phone;
Details of itemised calls from 1 telephone number which identified that the trader was deliberately not making any calls from the telephone number that he had provided to customers;

The data from these applications was not of benefit, so the investigation could not be progressed.

3.4 **Office of Surveillance Commissioners ('OSC') Inspection**

3.4.1 On 6th June 2013 an inspector from the Office of Surveillance Commissioners carried out an inspection of the Council's compliance with the directed surveillance and CHIS aspects of RIPA.

3.4.2 The inspection went very well. The conclusion to the inspection report stated "The commendable high standards of compliance when using powers under the 2000 Act continue to be achieved by this Council. It is clear that the engagement of the Chief Executive, oversight by the Senior Responsible Officer (Paul Lucas), and the retention of a highly experience and competent Authorising Officer (Tony O'Leary) remains the formula for the standards being maintained. OSC recommendations receive early adoption which is reflected in prompt policy revision."

3.4.3 The report then made 3 recommendations as follows:

- Original authorisation records to be retained by Legal Services.
- Improved oversight of un-regulated surveillance activity; and
- CHIS authorisations to be person specific and supported by relevant risk assessment;

3.4.4 These recommendations have all been implemented in practice, but it was decided to wait until the Home Office completed its review of the Codes of Practice (see 3.5 below) before changing the Council's corporate RIPA policy to clarify the new approach.

3.4.5 During the feedback session that followed the inspection, the inspector made a few minor suggestions for further improvements. These suggestions also needed to be incorporated into the revised version of the RIPA policy.

3.5 **Changes to use of RIPA**

3.5.1 Following an earlier consultation process, in July 2014 the Home Office published slightly revised versions of their Codes of Practice for directed surveillance and for the use of a CHIS. The main aspect of these changes is to incorporate the requirements for judicial approval that were introduced in 2012-13 which were previously reported to Members, and require further information to be recorded on the central register. Further clarification was also provided on some issues concerning circumstances when RIPA could be used by a local authority. The remaining changes do not relate to work carried out by local authorities.

3.5.2 Minor amendments are now required to be made to the Council's corporate RIPA policy to reflect the changes made to the Home Office Codes of Practice and also to implement the changes arising from the Office of Surveillance Commissioners' inspection as outlined in paragraph 3.4 and 3.5.1 above.

3.6 **Acquiring of Communications Data**

3.6.1 The Authority has received communication from the Interception of Communications Commissioner's Office (IOCCO) highlighting a general increase across England and Wales in the number of applicant errors arising as a result of applicants entering the wrong communications address (such as email addresses, telephone numbers) onto the application. In those cases the applicant error led to communications data being acquired relating to members of the public who had no connection to the investigation or operation being undertaken.

3.6.2 The SRO is responsible for oversight of the reporting of errors to IOCCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.

3.6.3 In light of the above the Council's corporate policy on the Acquiring of Communications Data has been amended to incorporate a statement that applicants are required to electronically copy (rather than manually) communications addresses into applications when the source is in electronic form (for example forensic reports relating to mobile phones, call data records etc) and that communications addresses acquired from other sources must be properly checked to reduce the scope for error.

3.6.4 In addition the UK Government recently announced that it intends to introduce legislation to ensure that Local Authorities only access communications data via the NAFN (National Anti Fraud network. Appropriate amendments have therefore been made to the policy to reflect the position as if this has come into effect as in practice Officers only use the NAFN route.

3.6.5 Finally the senior responsible officer role under this policy is currently allocated to Chris Jones (Service Director, Legal and Democratic Services), whereas Paul Lucas is the SRO for the rest of RIPA. In the interests of

consistency it is therefore makes sense to designate Paul Lucas as the SRO for all RIPA matters and the policy has been amended to reflect this change accordingly.

4. CONCLUSIONS

4.1 The Senior Responsible Officer considers that RIPA has been used sparingly and appropriately in relation to all of the above uses of directed surveillance or the acquiring of communications data and that RIPA has been used in a manner that is consistent with the two corporate policies. The most recent OSC inspection has confirmed this. In addition there has not been a requirement to make use of a CHIS during the period.

4.2 The Senior Responsible Officer also considers that the proposed revisions to the directed surveillance (RIPA) corporate policy, as attached at Appendix 1 to the report, and the policy on the acquiring of communications data, as outlined above and attached at Appendix 2, will ensure that both policies remain fit for purpose.

RHONDDA CYNON TAF
COUNTY BOROUGH COUNCIL

CORPORATE POLICY & PROCEDURES DOCUMENT

ON

THE REGULATION OF INVESTIGATORY

POWERS ACT 2000 (RIPA)

Paul J Lucas
Director of Legal and Democratic Services,
The Pavilions,
Cambrian Park,
Clydach Vale
Tonypandy

Adopted on: **21st July, 2004**

Revised: **June 2005, September 2006, May 2007, May 2010, December 2010, February 2013 and August 2014**

CONTENTS PAGE

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 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 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 and its Code of Practice. RIPA 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 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, 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 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 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 Act 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 Freedom 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 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)*

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 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);

- 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 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. 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.

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 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 will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

11. 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	a) Police Officer or Parks Warden on patrol; b) Signposted or clearly visible Town Centre CCTV cameras (in normal use); c) Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists; d) Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	a) CCTV or ANPR cameras providing general traffic, crime or public safety information. b) General observation duties forming part of the legislative functions of officers, as opposed to pre-planned surveillance of a specific person or group
Directed (must be RIPA authorised.)	a) Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit; b) 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. (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) c) CCTV or ANPR cameras used in a covert and pre-planned manner as part of a specific investigation
Intrusive **(the Council cannot do this!)**	a) Planting a listening or other device (bug) in a person's home, hotel room or in their private vehicle.

	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
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 directed or intrusive	a) Use of a recording device by a CHIS where this is allowed by the CHIS authorisation; b) Overt or covert recording of a voluntary interview with a member of the public by a local authority officer c) Covert recording of noise nuisance where the recording device records only excessive noise levels

Activity which should properly be authorised but which is not should be reported to the Office of the Surveillance 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 directed 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.

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.

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 require 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 s 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 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 directed 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 risk assessment form 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, 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 directed surveillance. A combined authorisation can be given for a CHIS and also directed 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) will not normally capture private information and, therefore, does not require authorisation.

    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 directed 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 directed 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.

Social Networking Sites and Internet Sites

17. 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.

18. 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.

19. 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.

20. 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.

H. Authorisation Procedures

1. Directed surveillance 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 on the Authorisation Form outlining:

- The activities to be authorised;
- The identities, where known, of those to be the subject of any directed surveillance;
- 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 directed 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)
- 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.

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.

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.

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. The Codes of Practice give some helpful examples to provide guidance on various points. 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. Proper 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 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:-

- Constitutes one or more criminal offences;

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;

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;

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:-

- 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 authorising 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 application form?

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;

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.

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 directed surveillance must be authorised by the 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;

(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 application form has been identified with a Unique Reference Number that the Applicant has obtained from the appropriate Co-ordinator in that service area.

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 eg PCHIS001, PCHIS002.

(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.

(h) The Authorising Officer should also record whether or not they are directly involved in the investigation.

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 directed 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 magistrate.

(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 application form (Form JA1) and prepare a Judicial Approval Order form (Form JA2) for signature by the Justice of the Peace (JP) The application 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 judicial application and order 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 judicial application and order 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 directed surveillance has been met.
The 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 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 form. This will be the official record of the JP's decision. Court staff will retain a copy of the RIPA authorisation and the judicial application and order forms. 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 authorisation;

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) Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form 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.

(j) 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 judicial application and order forms after they have been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

(k) 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 judicial application and order forms 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.

(l) 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.

(m) 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.

17. 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 authorisation) for Directed Surveillance, and 12 months (from authorisation) 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 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.

I. 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 directed 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) wish 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, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Service Director for 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) wish 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 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 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.

J. 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.

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. These records should be kept for 5 years.

Central Register maintained by the Senior Responsible Officer

5. Authorising Officers must forward the original authorising form (and any review / renewal / cancellation and rejection of the same) plus a copy of any judicial approval order form 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

6. The Central Record for directed surveillance will consist of:

- Date 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 magistrates' court 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

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

8. **Gatekeeper Role**

As a number of different Authorising Officers are entitled to authorise the use of directed surveillance 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

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

K. 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), identification of causes of errors and implementation of processes to minimise repetition of errors
- Engaging with OSC inspectors when they conduct inspections;
- Overseeing the implementation of any post-inspection action plans recommended by the OSC;

The Director of Legal and Democratic Services is the Senior Responsible Officer with regard to the use of directed surveillance or the use of a CHIS.

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 Commissioners

The Office of Surveillance Commissioners 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.

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.

L. 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 form and the 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 Lucas,
Director Legal and Democratic Services
The Pavilions,
Cambrian Park,
Tonypandy.
CF40 2XX

Tel: (01443) 424105
Fax: (01443) 424114
E-mail: paul.j.lucas@rhondda-cynon-taff.gov.uk

APPENDIX 1

List of Authorising Officer Posts

GROUP	Name of Contact Officer
CHIEF EXECUTIVE *Authorising Officers:* Chief Executive Director of Regeneration and Planning	 - Steve Merritt - Jane Cook
CORPORATE SERVICES *Authorising Officers*: Director of Legal and Democratic Services Service Director, Legal and Democratic Services Principal Solicitor Solicitor Head of Reviews and Benefits Team Manager Benefits	 - Paul Lucas - Chris Jones - Paul Nicholls - Simon Humphreys - Andrew Symes - Helen Phillips
ENVIRONMENTALSERVICES *Authorising Officers*: Service Director, Public Health & Protection Head of Community Protection Environmental Protection Manager Community Safety Manager Trading Standards Manager Housing and Enforcement Project Manager Food and Health and Safety Manager Pollution Manager Licensing Manager	 - Paul Mee - David Jones - Louise Davies - Andrew Mallin - Tony O'Leary - Jennifer Ellis - Amy Lewis - Neil Piliner - Meryl Williams
Service Director Planning Manager Special Projects Planning Enforcement Manager Car Parks and CCTV Manager Service Director for Streetcare Head of Streetcare	- Simon Gale - Jim Bailey - Julie Williams - Philip Shelton - Nigel Wheeler - Steve Owen

IMPORTANT NOTES

A. All persons employed in the posts identified above must receive appropriate training.

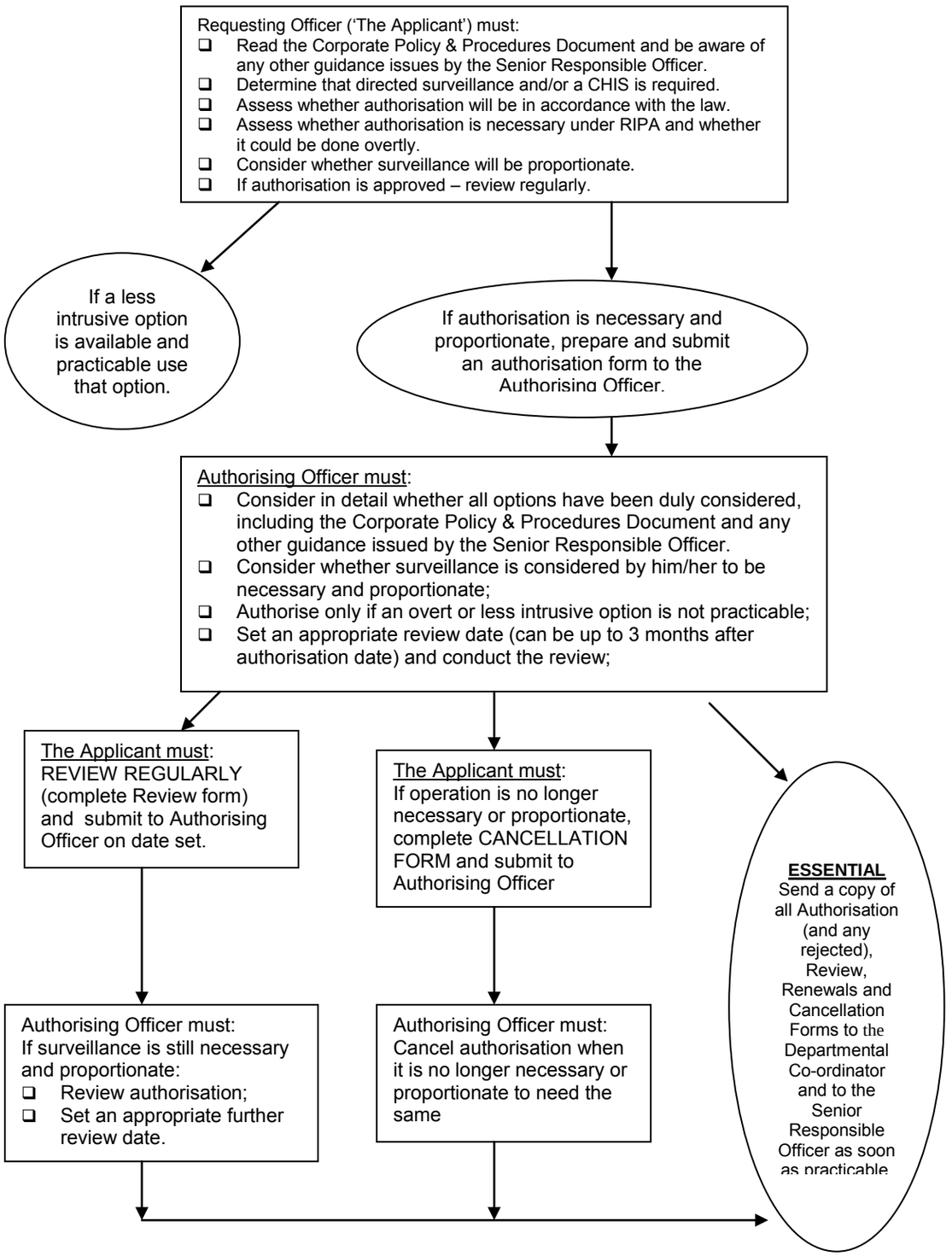
B. Only the Head of Paid Service is authorised to sign Forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph **G** of this Document).

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 directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

APPENDIX 2

RIPA FLOW CHART



NB: If in doubt, ask the Senior Responsible Officer BEFORE any directed surveillance 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 directed 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 directed 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 directed 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 directed 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 directed 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 directed 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 directed 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 CHIS or a directed surveillance 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 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 and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. A directed surveillance authorisation should be sought.

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 directed 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 directed 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 directed 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 directed 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 directed 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 directed 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 directed surveillance 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 directed surveillance authorisation and the authorising officer should consider the necessity and proportionality of conducting directed surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that directed surveillance 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.

Updating authorisations by review

Example 1
A directed 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 directed 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 directed 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 he has witnessed in his neighbourhood. The member of the public would not be regarded as a CHIS. He is 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 he is 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 his 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 directed surveillance.

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 directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

DS1

Directed Surveillance Unique Reference Number (URN)	

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

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Public Authority **(Including full address)**	

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

Details of application:

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No 521.[1]

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

Directed Surveillance Unique Reference Number (URN)	

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.

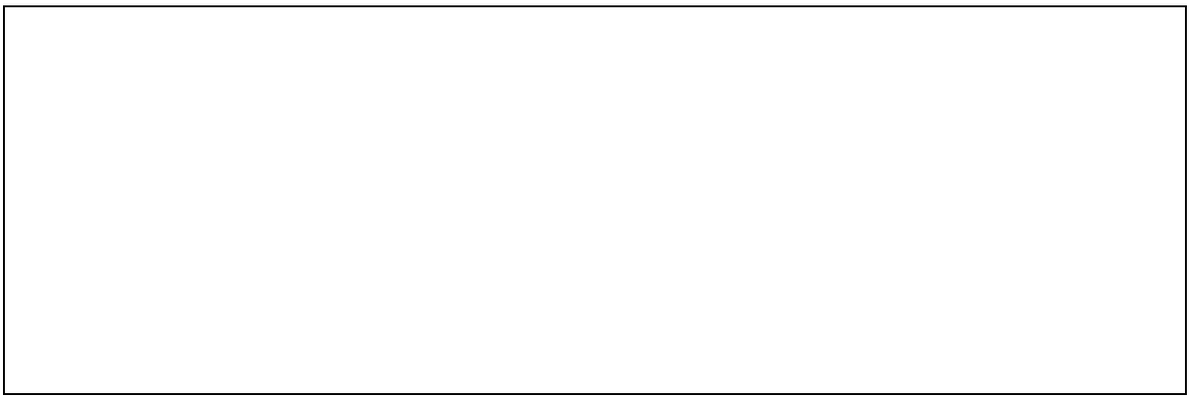
4. The identities, where known, of those to be subject of the directed surveillance.
• Name: • Address: • DOB: • Other information as appropriate:

Directed Surveillance Unique Reference Number (URN)	

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 <u>necessary</u> 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, 147or 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933 **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 <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3]



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 3.8 to 3.11]
Describe precautions you will take to minimise collateral intrusion

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraphs 3.4 to 3.7]

Directed Surveillance Unique Reference Number (URN)	

10. Confidential information. [Code paragraphs 4.1 to 4.31] INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising officer's statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.]
I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

Directed Surveillance Unique Reference Number (URN)	

13. Explain <u>why</u> you believe the directed surveillance is necessary. [Code paragraph 3.3] **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraphs 3.4 to 3.7]**

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

Date of first review	

Directed Surveillance Unique Reference Number (URN)	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
Name (Print)		**Grade/Rank**		
Signature		**Date and time**		
Justice of the Peace granting Judicial Approval		**Date and time of judicial approval**		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 – expires on 30 June 2005, 23:59]				

15. Is Authorising officer directly involved in this Investigation/Operation?
YES/NO

Directed Surveillance Unique Reference Number (URN)	

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				
Name (Print)		**Grade/Rank**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		

Remember the 72 hour rule for urgent authorities – check Code of Practice	e.g. authorisation granted at 5pm on June 1st expires 4:59pm on 4th June		

DS 2

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)

Public Authority *(including full address)*	

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

Details of Renewal:

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

Directed Surveillance Unique Reference Number (URN)	

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.

Directed Surveillance Unique Reference Number (URN)	

7. Applicants Details			
Name (Print)		**Tel. No.**	
Grade/Rank		**Date**	
Signature			

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

9. Authorising Officer's Statement.
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.
Name (Print) …… Grade/Rank…… **Signature …… Date ……..**

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

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

DS 3

Directed Surveillance Unique Reference Number (URN)	

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

REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority *(including full address)*	

Applicant		**Unit/Branch/ Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number* *Filing Ref**	
Date of Authorisation or Last Renewal		**Expiry Date of Authorisation or Last Renewal**	
		Review Number	

Details of Review:

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

Directed Surveillance Unique Reference Number (URN)	

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.

Directed Surveillance Unique Reference Number (URN)	

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

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

9. Authorising Officer's Statement.
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal] [it should be cancelled immediately).
Name (Print) …… Grade/Rank…….. **Signature …… Date ……..**

10. Date of next review.	

DS 4

Directed Surveillance Unique Reference Number (URN)	

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

CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION

Public Authority *(including full address)*	

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

Details of cancellation:

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

Directed Surveillance Unique Reference Number (URN)	

2. Explain the value of surveillance in the operation:

3. Explain the outcome that was obtained from using the surveillance:

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:

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

6. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

7. Authorisation cancelled.	**Date:**	**Time:**

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.

Form CHIS 1

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)

Public Authority *(including full address)*	

Name of Applicant		**Service/Department/ Branch**	
How will the source be referred to? i.e. what will be his/her pseudonym or reference number			
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)?			

Investigation/Operation Name (if applicable)	

Details of application:

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No. 521[1].

CHIS Unique Reference Number (URN)	

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail <u>the purpose</u> for which the source will be tasked or used. Please explain how achieving this purpose will assist the investigation.

[1] 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.

4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used

5. Identify on which grounds the conduct or the use of a source is <u>necessary</u> 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 <u>why</u> this conduct or use of a source is necessary on the grounds you have identified [Code paragraph 3.2]

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11] **Describe precautions you will take to minimise collateral intrusion and how any will be managed.**

8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source (see Code paragraphs 3.17 to 3.18)?
9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.14).
10. Explain <u>why</u> 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 to 3.5]

CHIS Unique Reference Number (URN)	

11. Confidential information [Code paragraph 4.1 to 4.21] Indicate the likelihood of acquiring any confidential information

12. Applicant's Details			
Name (Print)		**Grade/Rank/ Position**	
Signature		**Tel No:**	
Date			

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

CHIS Unique Reference Number (URN)	

14. Explain <u>why</u> you believe the conduct or use of the source is necessary. [Code paragraph 3.2] **Explain <u>why</u> you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement. [Code paragraphs 3.3 to 3.5]**
15 (Confidential Information Authorisation). Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.21

16. Date of first review:	

CHIS Unique Reference Number (URN)	

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

18. Authorising Officer's Details			
Name (Print)		**Grade/Rank/Position**	
Signature		**Time and date granted** **Time and date authorisation ends**	
Justice of the Peace granting judicial approval		**Time and date of judicial approval**	

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?
YES/NO

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.

CHIS Unique Reference Number (URN)	

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				
Name (Print)		**Grade/Rank/ Position**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72 hour rule for urgent authorities – check Code of Practice [Code Paragraph 4.18]. e.g. authorisation granted at 17:00pm on 1st June 2006 expires 16:59pm on 4th June 2006.				

Form CHIS 2

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)

Public Authority *(including full address)*	

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

Details of renewal:

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

CHIS Unique Reference Number (URN)	

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.

CHIS Unique Reference Number (URN)	

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

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

CHIS Unique Reference Number (URN)	

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

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

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

CHIS 3

Operation Reference Number* **(Filing Ref)**	

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

CANCELLATION OF AN AUTHORISATION FOR THE USE OR CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

Public Authority *(including full address)*	

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

Details of cancellation:

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

Operation Reference Number* (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			
Name (print)		**Grade:**	
Signature		**Date**	

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

Date:		**Time:**	

7. Authorisation cancelled.	**Date:**	**Time:**

(Form CHIS 4)

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.	

Form CHIS 5

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

Public Authority *(including full address)*	

Applicant		**Unit/Branch/ Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number* *Filing Ref**	
Date of Authorisation or Last Renewal		**Expiry Date of Authorisation or Last Renewal**	
		Review Number	

Details of Review:

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

CHIS Unique Reference Number (URN)	

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.

CHIS Unique Reference Number (URN)	

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

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

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

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

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.

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:

RHONDDA CYNON TAF
COUNTY BOROUGH COUNCIL

CORPORATE POLICY & PROCEDURES DOCUMENT

ON

THE ACQUISITION OF COMMUNICATIONS DATA UNDER

REGULATION OF INVESTIGATORY

POWERS ACT 2000 (RIPA)

Paul J Lucas
Director of Legal and Democratic Services,
The Pavilions,
Cambrian Park,
Clydach Vale
Tonypandy

Adopted on 10th March 2008
Revised August 2008, December 2010,February 2013 and September 2014

CONTENTS PAGE

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 Practice on the Acquisition and Disclosure of Communication Data. 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 for advice and assistance. Appropriate training and development will be organised by the Senior Responsible Officer to relevant Authorising Officers and other senior managers.

3. Copies of this Document and related Forms will be placed on the Intranet.

4. The Senior Responsible Officer has authorised the Council's Lead Officer for RIPA and Accessing Communications Data to maintain the Corporate Register of all RIPA communications data forms, but this register will be subject to examination by the Senior Responsible Officer as and when it is deemed necessary. It is the responsibility of the relevant Authorising Officer, however, to ensure that the Lead Officer receives a copy of the relevant Forms as soon as practicable.

5. RIPA and this Document are important for the effective and efficient operation of the Council's actions with regard to acquiring communications data. This Document will, therefore, be kept under review by the Senior Responsible Officer. 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.

6. 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.

Effective Date of Operation And Authorising Officer Responsibilities

1. The Corporate Policy, Procedures and the Forms provided in this Document became operative with effect from the date of its adoption by the Council, that is 10th March 2008. After adoption no other Forms are allowable. 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. Chief Officers have designated Authorising Officers within the appropriate divisions to take action under RIPA. These persons are detailed in the Corporate Policy and Procedures Document on Regulation of Investigatory Powers Act and as Authorising Officers they are entitled to act as Designated Persons for acquiring communications data.

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 obtaining of communications data without first obtaining the relevant authorisations in compliance with this Document.

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

ACQUISITION OF COMMUNICATIONS DATA

Introduction

Part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000 controls the acquiring of communications data by Local Authority staff. Communications data does not include the content of the communications such as the e-mail message, the letter or text, or the content of the phone call.

Part I introduces a statutory framework to regulate access to communications data by public authorities consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights, in order to balance the rights of the individual against the needs of society as a whole to be protected from crime and other public safety risks.

The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the ECHR only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with the law.

As a result officers should not require, or invite, any postal or telecommunications operator to disclose communications data either by using other statutory powers or by exercising any exemption to the principle of non-disclosure under the Data Protection Act 1998.

What is Communications Data and what categories are there?

Communication data means any traffic or any information that is or has been sent over a telecommunications system or postal system, together with information about the use of the system made by any person. In effect the term communications data embraces the "who, when and where" of a communication but not the content, not what was said or written. It includes the manner in which and by what method a person (or machine) communicates with another person (or machine), but excludes what they say or data they pass on, including text, audio and video. Content is covered by Interception of Communications legislation.

An operator who provides a postal or telecommunications service is described as a Communications Service Provider (CSP).

RIPA defines communications data in three broad categories: -

(a) **Section 21(4)(c) Information about communications service users**
This category mainly includes personal records supplied to the Communication Services Provider (CSP) by the customer/ subscriber. For example, their name and address, payment method, contact number etc.

(b) **Section 21(4)(b) Information about the use of communications services**
This category mainly includes everyday data collected by the CSP related to the customer's use of their communications system and which would be routinely available to the customer. For example, details of the dates and times they have made calls and which telephone numbers they have called.

(c) **Section 21(4)(a) Information about communications data (traffic data)**

This category mainly includes data generated by the Communications Service Provider (network data) relating to a customer's use of their communications system (that the customer may not be aware of), for example, cell site data and routing information.

Communications Data that can be acquired

The types of information that we are allowed to access from a CSP fall into 2 categories.

Subscriber Information (RIPA S 21(4)(c)) - Information about communications services users

- Name of the customer who is the subscriber for a telephone number, an e-mail account, PO Box number, a Post Paid mailing stamp, or is entitled to post to a web space;
- Account information such as address for billing, delivery or installation;
- Subscriber account information such as bill paying arrangements, including details of payments and bank or credit/ debit card details;
- Information about the provision of forwarding and redirection services;
- Information about connection, disconnection and reconnection of services the customer subscribes to, including conference calling, call messaging, call waiting and call barring telecommunications services;
- Information provided by the subscriber to the CSP such as demographic information or sign up data (other than passwords) such as contact telephone numbers;
- Information about telephones or other devices provided by the CSP to the subscriber and associated codes, including Personal Unlocking Keys for mobile phones & serial numbers;

Service Use Data (RIPA S 22(4)(b) – Information about the use of communications services

- Periods during which the customer used the service;
- Activity including itemised records of telephone numbers called, Internet connections, dates and times of calls, duration of calls, text messages sent and quantities of data uploaded or downloaded;
- Information about use made of forwarding and redirection services;
- Information about the use made of conference calling, call messaging, call waiting and call barring telecommunications services;
- Information about the selection of preferential numbers or discount calls;
- Records of postal items, such as records of registered, recorded or special delivery postal items and records of parcel consignment, delivery and collection;
- Top-up details for pre-pay mobile phones including credit/ debit card, voucher/ e-top up details;

Traffic data (RIPA S 22(4)(a) – Information about the communications themselves

NB We are NOT allowed to access traffic data

Traffic data includes

- Information identifying the sender and recipient of a communication;
- Information tracing the origin or destination of a communication including incoming call records;
- Information identifying any location of any equipment making a communication, such as mobile phone cell site location;
- Web browsing information such as web sites visited or servers used;
- Addresses or markings, including sender or recipient, written on the outside of a postal item in transmission (such as a letter or parcel), that shows the items postal routing;
- Online tracking of communications such as postal items;

NB Local Authority staff are only allowed to acquire and disclose communications data for the purpose of preventing or detecting crime or of preventing disorder;

There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Service Providers").

In order to compel a Communications Service Provider to obtain and disclose, or just disclose communications data in their possession, a notice under S22 (4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice is likely to be the main power utilised by us, in those circumstances where the Council SPOC liaises directly with the Communications Service Provider.

In addition S22 (3) provides that a Designated Person can authorise another person within the same relevant public authority to engage in specific conduct to collect the data. This allows the local authority to collect the communications data themselves, e.g.. if a Communications Service Provider is technically unable to collect the data, an authorisation under this section would permit the local authority to collect the communications data themselves. Commonly this will occur if there is an agreement in place between a public authority and a CSP relating to appropriate mechanisms for disclosure of communications data directly to the authority. The authorisation describes the conduct that is authorised and describes the communications data to be acquired by that conduct. Where a SPOC has been authorised to obtain subscriber details but then concludes that the data is held by a CSP from whom it cannot be acquired directly, rather than obtaining a notice, the SPOC can provide the CSP with details of this authorisation in order to seek disclosure of the required data.

However it is relatively unlikely that the Council will directly issue any authorisations ourselves, as the majority of the Communications Service Providers will have sufficient resources in place to allow them to collect the information following the service of a S22 (4) Notice. However the Council may need to issue authorisations when using the streamlining process to widen data capture when trying to identify the user of a prepaid mobile phone. By contrast, when they are acting on our behalf the SPOCs for the National Anti Fraud Network (NAFN) usually operate via the authorisation process, as they are then able to obtain the data themselves by directly interrogating the CSP databases.

How to obtain Communications data

There are two different methods that officers can use to obtain communications data.

1. The original method is by means of paper forms being completed by the Applicant, then the application being approved by the Designated Person and finally the notices being sent by the Single Point of Contact (SPOC) to the relevant Communications Service Provider via fax or e-mail. In due course the CSP sends the required communications data to the SPOC and it is then passed to the Applicant. The Government now requires that local authorities cease to use this method, so the forms relating to the use of this method have been removed.
2. The second method is by means of the National Anti Fraud Network (NAFN) secure website. To use this system Applicants have to individually register on the NAFN website at www.nafn.gov.uk. Once registered the Applicant completes the application form online and it is then submitted electronically to one of the SPOCs at NAFN, who will advise the Applicant of any need for changes. The Designated Person then receives an e-mail to say that there is an application form on the website for him or her to consider and the Designated Person completes the relevant part of the form to provide his or her decision. The NAFN SPOC then uses the authorisation process to obtain the required communications data from the CSP database and that data is posted on the website so that

it can only be accessed by the Applicant. If NAFN do not have direct access to the database of the relevant CSP their SPOC will send a notice to the CSP in the usual way.

Using the NAFN website method has significant advantages over using the Council SPOC method as a) the turn round times for obtaining the communications data are considerably reduced, b) the costs charged by the CSPs for providing the data are considerably less when using NAFN and c) it ensures consistency across all Designated Persons and Local Authorities when acquiring communications data.

Consequently, from December 2010 onwards, Applicants will be expected to use the NAFN website for all applications for communications data. From the implementation of the September 2014 policy we will no longer be allowed to use the paper-based system.

Applying for Communications data

As with other RIPA issues, the investigating officer who needs to acquire communications data (the Applicant) must complete an application form. This is the online NAFN form). The online forms require the officer to complete a declaration before submitting the form to NAFN.

On this form the Applicant must provide information about:

- Name and designation of Applicant;
- The purpose for which the data is required, which can only be for the prevention and detection of crime;
- Details of the communications data required;
- Outline the source of the communications data address(es) (in the necessity section)
- Time period for which the data is required, including historic or future data;
- Why it is necessary to obtain the data and what is expected to be achieved from obtaining it;
- Why it is proportionate for the data to be obtained, including why the intrusion benefits the investigation and whether the level of intrusion can be justified against the individual's right to privacy;
- Details of whether there is any meaningful collateral intrusion and why that intrusion is justified;

Timescale within which the data is required, which can only be the "routine non-urgent" timescale" i.e. Grade 3, unless there is a high level of urgency for obtaining the data, such as when life is in danger;

- The applicant also confirms that he or she will undertake to inform the SPOC of any changes in circumstances that no longer justify the acquisition of the data;

It is good practice for the Applicant to mention on the Application Form if they have carried out any open source checks on the telephone numbers or other communications addresses that are under investigation, as this assists with justifying the principle of proportionality

The Applicant is entitled to ask for historical data or may request future data, by which the Communications Service Provider must provide details of, say all outgoing telephones or Internet connections over a set future period of up to a month. Requests for such future data are considered to be more intrusive than requests for historical data.

The form is then passed electronically to the appropriate NAFN accredited Single Point of Contact for Accessing Communications Data (SPOC).

It can be appropriate to obtain service use data at the same time as obtaining subscriber information, for example when the person who is the subject of the investigation is identified from

high-grade intelligence to be using a specific number or service or when a mobile phone is lawfully seized. An application for subscriber information can be included in an application for service use data.

Prepaid Mobile Phones
Subscriber checks on some mobile telephone numbers may reveal that the phone is an unregistered prepaid mobile telephone as these types of phones are used by many criminals to avoid detection. However, in order to gather more information, the Applicant making a request is able to ask for further information about the subscriber under section 21(4)(c) including top-up details, method of payment, bank account used or customer notes. The Applicant should outline in their original application the further information that will be required if the phone turns out to be prepaid, so as to allow the widening of the data capture. This information could be requested in two stages: firstly asking for the subscriber details and then, if this turns out to be an unregistered prepaid phone, asking for the further information. If the Designated Person approves the application it is recommended by IOCCO that he or she should approve the use of authorisations rather than the use of notices, whereby the authorisation should state that the SPOC is authorised to engage in any conduct to acquire information about the user that is covered by Section 21(4)(c). Under the legislation an authorisation does not have to be issued by the Designated Person so it can be issued by the SPOC. The SPOC will then serve an appropriate authorisation on the relevant Communications Service Provider. If further information is required the SPOC will need to serve another authorisation on the CSP requesting the additional information. It should be noted that each authorisation will bear the date that the Designated Person approved the original application. This streamlining process is more efficient than using notices, because otherwise a request for each additional notice would need to be referred to the Designated Person.

The information that is received can then be developed to try to obtain further information about the user of the phone. Solution Providers such as EasyPay, EPay etc, are the third parties involved in the transaction of credit placed on a mobile phone. If a Solution Provider is provided with the mobile telephone number, the transaction date and the transaction number, they are often able to provide the method of payment and the location of the top-up. Solution Providers are not CSPs and therefore they cannot be issued with a notice under RIPA; instead the data can be applied for under the Data Protection Act.

Home Office Guidance on completing the forms
The Home Office has provided guidance on the forms namely “Guidance for the layout of a Chapter II application form and guidance for Applicants and Designated Persons considering necessity and proportionality”. The guidance was produced jointly by the Home Office and the Data Communications Group (DCG) in conjunction with the Interception of Communications Commissioner’s Office. The full document is available from the SPOC but these are the relevant extracts from it

Home Office Guidance on Communications Data

An application, comments by the Single Point of Contact (SPOC) considerations of the Designated Person, authorisations and notices may be made in writing (“paper”) or electronically (“database”).

It may be appropriate for the section “communications data” to include “text boxes” to enable the applicant to set out the:

- Telephone number, email address, etc;
- Where appropriate the ”between times/ dates” of the data set required;
- Type of data required, for example subscription details, outgoing calls, incoming calls;

An application may contain several requests for various “data sets” relating to a specific investigation or operation. However, consideration should be given as to how this may affect the

efficiency of the public authority's processes and the impact of managing disclosure issues before, during and after a criminal trial.

Home Office Guidance on Necessity

In order to justify the application is necessary the applicant needs to consider three main points:

- Crime/ offence/ circumstance ("the **event**") under investigation;
- Subject(s)/ offender(s)/ witness(es)/ victim(s) ("the **person**") and how the person(s) is/are linked to the event;
- Telephone number(s), IP address(es) etc ("the **communication**") and how this/ these relate or link the person and the event;

Sensitive sources of intelligence or covert investigation techniques may be referred to in the application but the Applicant must be mindful of the appropriate security handling of the application once completed. It may be sufficient to refer to an intelligence reference number within the body application dependent on the security issues involved.

The information given by the Applicant (which includes "background information" or the "intelligence case") should be set out within an application under the headings of **necessity** and **proportionality** (which includes the consideration of meaningful collateral intrusion). This will minimise the need to repeat information within an application and enable the process to be streamlined.

In essence, necessity should be a short explanation of a) the event, b) the person and c) the communication and how these three link together.

The application must establish a link (which may, where justified, include an inferential link) between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

A brief description of the investigation or operation may assist the Designated Person better understand the reason for the application.

In a long term or complex investigation or operation it is important to set the application in context with the overall investigation or operation and set the scene and background, which then leads into the Applicant's specific investigative or operational requirements (which should be covered in the proportionality section)

Necessity <u>does not</u> entail explaining "what will be achieved by acquiring the data" or "why specific time periods have been requested" – these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

Home Office Guidance on Proportionality

Applicants should outline how obtaining the data will benefit the investigation or operation. The two basic questions:

- "What are you looking for in the data to be acquired?"
- "If the data contains what you are looking for, what will be your next course of action?"

The relevance of any time periods requested must be explained outlining how these periods are proportionate to the event under investigation.

An explanation as to how communications data will be used, once acquired, and how it will benefit the investigation or operation, will enable the Applicant to set out the basis of proportionality.

An investigation or operation which is seeking to acquire several sets of traffic data or service use data should engage with the SPOC to develop strategies (or collection plans) to obtain the communications data and the detail of that strategy may be included within the application (see paragraph 3.17 of the code).

Home Office Guidance on Collateral Intrusion

Collateral intrusion forms party of the proportionality considerations and becomes increasingly relevant when applying for traffic data or service use data. Applicants should outline specifically what collateral intrusion may occur, how the time periods requested impact on the collateral intrusion, whether they are likely to obtain data which is outside the realm of their investigation and outline their plans for managing it., for example during the course of an investigation. To establish certain facts it may be necessary and proportionate for an investigator (Applicant) to require access to communications data that relates to witnesses as well as the associates of a suspect or target.

The question to be asked is "Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for? For example due to the very specific nature of telephone number subscriber check(s), collateral intrusion on a person other than the subscriber detail(s) will be consistently absent ,whereas itemised billing on the subject's family home will be likely to contain calls made by the family members.

Applicants should not write about a potential or hypothetical "error" and if the Applicant can not identify any meaningful collateral intrusion that factor should be recorded in the application i.e. "none identified".

Home Office Guidance on time scale

Completion of this section assists the SPOC to prioritise the request

DCG has an agreed Grading System that indicates to the CSP any urgent timescales, which is synchronised with the Urgent Oral Process (see footnote 40 and paragraph 3.56 of the code)

Role of the SPOC

The Home Office must accredit all SPOCs, and this involves attendance on a recognised training course, the passing of an examination and being issued with a SPOC Personal Identification Number. The SPOC ensures that only practical and lawful requests for communications data are undertaken.

All notices and authorisations for communications data must be channelled through the SPOC. This is in order to provide an efficient regime since the SPOC will deal with the Communications Service Providers on a regular basis.

The SPOC will receive the application form and will advise Applicants and Designated Persons on:

- Whether the forms have been filled in correctly and are lawful;
- Whether the data requested falls within Section 21(4) (a), (b) or (c) of the act;
- Whether access to the communications data is reasonably practical for the Communications Service Provider or whether the specific data required is inextricably linked to other data;
- The practicalities of accessing different types of communications data from different telecommunications or postal operators;

- Whether data disclosed by a CSP fulfils the requirements of the notice;

The SPOC will assess the Application for Communications Data form and on it record:

- If the request is not reasonably practical for the SPOC the reason why this is so;
- Whether the data falls into Section 21(4) (a), (b) or (c) of the act;
- Whether a notice or authorisation is appropriate;
- Any adverse cost implications to the CSP or local authority;
- Details of any data that is likely to be obtained in excess of the data requested;
- Any other factors that the Designated Person should be aware of;
- Description of the data to be acquired and, where relevant, specifying whether any historic or future data is required and the time periods sought;
- Identifying the relevant Communications Service Provider;

The SPOC will issue a Unique Reference Number for the form. The SPOC will draft the relevant notice or authorisation to be submitted for approval to the Designated Person. The SPOC will keep a chronological record of the processing of the application including any contacts made by him or her with the Communications Service Providers. He or she may also give a priority grading to the CSP depending on the urgency of the application.

NAFN employ a number of officers as SPOCs and they can be contacted on 01273 291660 in order to discuss any issues.

Home Office Guidance on considerations of the SPOC

If the application is being recorded within a database (or other electronic format), and is attributable to the applicant, a signature is not required.

An application, comments by the single point of contact (SPOC), considerations of the Designated Person, authorisations and notices may be made in writing (“paper”) or electronically (“database”).

The question “Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought”, is appropriate where the communications data sought by the Applicant may need refinement by the SPOC, for example incoming calls to a telephone number held by a CSP that does not keep a data set that can reveal such calls. The SPOC would state that several authorisations and notices will need to be undertaken with CSPs that can reveal calls instigating from the networks to the telephone number in question.

The Designated Person, having considered the comments of the SPOC, may decide the acquisition is not justified because of the significant resources required by the CSP to retrieve and disclose the data or it will be impractical for the public authority to undertake an analysis of the data.

It will also be appropriate for the SPOC to comment where the data sought by the Applicant will require the acquisition of excess data, specifically where it is not practicable for the CSP to edit or filter the data, for example a specific incoming call in a data set with outgoing calls and cell site contained in it. If the Designated Person considers this to be necessary and proportionate for the acquisition of the specific incoming call then the authorisation or notice must specifically include the acquisition of the outgoing call, incoming calls and cell site.

Approval by Designated Person

The SPOC will then submit the Application for Communications Data Form, along with the relevant draft notice(s) or authorisation(s), to a Designated Person, who will make the decision about

whether or not the application will be approved. The Designated Persons will be those officers, of a suitable rank, who are currently Authorised Officers under RIPA, so they are already able to approve surveillance or CHIS applications. In no cases may someone be both the Designated Person and the Applicant.

Designated Persons must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

The Designated Person will consider the form and then complete the Designated Person's part of the Application Form to state whether they grant or refuse the application. On the form the Designated Person must record:

- Why he/she believes acquiring the communications data is necessary;
- Why he/she believes the conduct involved in acquiring the communications data is proportionate;
- If accessing the communications data involves a meaningful degree of collateral intrusion, why he/she believes that the request is still proportionate;

The decision of the Designated Person must be based on the information presented to them in the application. If the application is approved the Designated Person can authorise the accessing of communications data by one of 2 different methods:

- By a notice under RIPA S 22(4), which is a notice given to the postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the Authority that served the notice.
- By an authorisation under RIPA S 22(3), which allows the Authority to collect and retrieve the data itself. (It is extremely unlikely that we will make use of this, as this is only intended to be used if the operator is incapable of complying with a notice, or if the Authority will retrieve the data using an on-line system.)

The Designated Person should specify the shortest time period for the data that is necessary in order to achieve the objective for which the data is sought.

The Designated Person shall endorse the draft notice or authorisation with the date, and if appropriate the time, at which he or she gives the notice or authorisation. This is the point at which the Designated Person approves the application.

If the Designated Person wishes for any advice they are able to obtain it from the SPOC.

Generally Designated Persons should not be responsible for approving applications in which they are directly involved. Therefore it is best practice for a manager from a service area not involved in the investigation to act as Designated Person for an application from the service area carrying out the investigation. However sometimes this is unavoidable, so in these cases this should be acknowledged and the manager's justification for undertaking the role of Designated Person in the investigation should be stated in their considerations.

If the application is rejected either by the SPOC or the Designated Person, the SPOC will retain the form and inform the applicant in writing of the reasons for its rejection. The NAFN SPOC will do so via the website.

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

Home Office Guidance on considerations of the Designated Person

The Designated Person must be able to show he or she has understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny.

The Designated Person should tailor their comments to a specific application as this best demonstrates the application has been properly considered.

If the Designated Person having read the application considers the Applicant has met all the requirements then he or she should simply record that fact. In such cases a simple note by the Designated Person should be recorded.

There may be circumstances where the Designated Person having read the case set out by the Applicant and the considerations of the SPOC will want to comment why it is still necessary and proportionate to obtain the data despite excessive data being acquired.

If the Designated Person does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPOC and the Applicant.

A notice must include a unique reference number that also identifies the public authority. This can be a code or abbreviation.

If the Designated Person is recording their considerations within a database (or other electronic format) and is attributable to the Designated Person, a signature is not required.

Notices and authorisations

The NAFN SPOC will supply the Designated Person with a draft notice or authorisation. Where a notice needs to be issued, the NAFN SPOC will produce the notice on behalf of the Designated Person All notices and authorisations should refer to data relating to a specific date or period of time. If the date is specified as “current” the data should be provided by the CSP as at the date of the notice. The notice should give enough information to the CSP to allow them to comply. There is no need to produce a separate notice for each communications address, when these addresses all relate to the same CSP.

The notice is then served on the Communications Service Provider by the relevant SPOC. The SPOC will give the notice a Unique Reference Number that cross-references it to the application that was granted. The SPOC is responsible for all contacts between the Authority and the Communications Service Provider.

Authorisations will mainly be utilised when carrying out the streamlining process for prepaid phones. The SPOC will generate the authorisation on behalf of the Designated Person. The NAFN SPOC will be able to obtain the communications data from the CSP database. Legally the authorisation does not need to be served on the CSP. However the CSP may require or be given an assurance that the conduct undertaken is lawful. That assurance may be given by disclosing details of the authorisation or by providing the actual authorisation.

Once the data is obtained the SPOC will provide the data to the Applicant, but the SPOC can filter out any unnecessary information provided by the Communications Service Provider. The SPOC will retain the original data obtained from the CSP (known as the “golden copy”) and provide a copy of it to the Applicant. This golden copy is capable of being provided to the CSP in the future, in order to enable a witness statement to be obtained in circumstances where the CSP no longer

retains their original data. The Applicant should keep the data that they receive in a secure manner, in order to comply with data protection requirements.

The Communications Service Provider must comply with the requirements of a notice, as long as it is reasonably practical for them to do so. Under S24 of RIPA the Communications Service Provider is entitled to recover the reasonable costs of making “timely disclosure” of such data. Ordinarily the CSP should disclose the required communications data within 10 working days of the notice being served on them, but if in specific circumstances where this would not be possible the Designated Person may specify a longer period of up to a month.

All notices and authorisations will only be valid for a month, but they may be renewed for further periods of a month, at any time within the current life of the notice or authorisation. This should be set out by the Applicant in an addendum to the original application.

If the need for the communications data ends or its obtaining is no longer proportionate before the provision of this data by the Communications Service Provider, the Designated Person must cancel the notice using a cancellation form, which is then sent to the CSP. In a similar manner an authorisation must be withdrawn and, if appropriate, the CSP should be advised of this withdrawal. In the NAFN system this is done via the website. However the notices (and authorisations) terminate when the Communications Service Provider provides the requested data, so there is usually no need for a cancellation form to be completed.

All original documents will be retained by the SPOC.

Judicial Approval

Once an application for the acquisition and use of communications data has been authorised by the Authorising Officer, the authorisation or notice then needs to receive judicial approval from a magistrate.

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 application form (Form JA1) and prepare a Judicial Approval Order form (Form JA2) for signature by the Justice of the Peace (JP) The application form will contain a brief summary of the circumstances of the case.

The officer will provide the JP with a copy of the original RIPA authorisation or notice 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 judicial application and order forms will be provided to the JP.

The hearing will be in private and will be heard by a single JP. The JP will read and consider the RIPA authorisation or notice and the judicial application and order forms. He or she may ask questions to clarify points or to require additional reassurance on particular matters.

The JP will consider whether he or she is satisfied that at the time the authorisation or notice was granted or renewed there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds.

The 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 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.

If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation or notice. 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.

The JP will record his/her decision on the Judicial Order form. This will be the official record of the JP's decision. Court staff will retain a copy of the RIPA authorisation and the judicial application and order forms. This information will be retained securely.

The decisions that the JP can make are as follows:

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

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

Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form 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 or notice, the court must not exercise its power to quash that authorisation or notice unless the Applicant has had at least 2 business days from the date of the refusal in which to make representations.

The Council will need to obtain judicial approval for all initial RIPA authorisations or notices as well as for all renewals and officers will need to retain a copy of the judicial application and order forms after they have been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

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 judicial application and order forms 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 the next working day.

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.

Errors

Where any error occurs, in the giving of a notice or authorisation or as a consequence of any authorised conduct or any conduct undertaken to comply with a notice, a record should be kept. An error can only occur after the notice has been served on the CSP, so if it is discovered before this point it does not officially count as an error.

There are 2 types of errors namely reportable errors and recordable errors.

- Reportable errors are ones where communications data is acquired wrongly and in this case a report must be made to the Interception of Communications Commissioner, as this

type of occurrence could have significant consequences for the individual whose details were wrongly disclosed.

- Recordable errors are ones where an error has occurred but has been identified before the communications data has been acquired. The Authority must keep a record of these occurrences, but a report does not have to be made to the Commissioner.

Reportable Errors could include:

- A notice being made for a purpose, or for a type of data, which the public authority cannot seek;
- Human error, such as incorrect transposition of information;
- Disclosure of the wrong information by a CSP when complying with a notice;
- Disclosure or acquisition of data in excess of that required;

Recordable Errors could include:

- A notice which is impossible for a Communications Service Provider to comply with;
- Failure to review information already held, e.g. seeking data already acquired or obtained for the same investigation, or data for which the requirement to obtain it is known to be no longer valid;
- Notices being sent out to the wrong Communications Service Provider;
- Notices being sent out to CSPs that were not produced by the Designated Person who authorised the application;

Where a telephone number has been ported to another Communications Service Provider then this does not constitute an error. Where excess data is disclosed, if the material is not relevant to the investigation it should be destroyed once the report has been made to the Commissioner. If having reviewed the excess material it is intended to make use of it, the Applicant must make an addendum to the original application to set out the reasons for needing to use this excess data. The Designated Person will then deicide whether it is necessary and proportionate for the excess data to be used in the investigation.

Any reportable error must be reported to the Senior Responsible Officer and then to the Commissioner within 5 working days. The report must contain the unique reference number of the notice and details of the error, plus an explanation how the error occurred, indicating whether any unintended collateral intrusion has taken place and providing an indication of the steps that will take place to prevent a reoccurrence. The Reporting an Error by Accredited SPOC Form (CD5) should be used for this purpose.

If the report relates to an error made by a Communications Service Provider the Authority must still report it, but should also inform the CSP to enable the CSP to investigate the cause.

The records kept for recordable errors must include details of the error, explain how the error occurred and provide an indication of the steps that will take place to prevent a reoccurrence. These records must be available for inspection by IOCCO inspectors and must be regularly reviewed by the Senior Responsible Officer.

The most common cause of errors is the incorrect transposition of telephone numbers, e-mail addresses and IP addresses. In the vast majority of cases these addresses are derived from addresses available to the Applicant in electronic form. Therefore all Applicants are required to electronically copy communications addresses into applications when the source is in electronic form (for example forensic reports relating to mobile phones or call data records etc.) Communications addresses acquired from other sources must be properly checked to reduce the scope for error.

Senior Responsible Officer

The Senior Responsible Officer is responsible for:

- The integrity of the processes of acquiring communications data;
- Compliance with the act and code of practice;
- Oversight of the reporting of errors to IOCCO;
- Engaging with IOCCO inspectors when they conduct inspections;
- Overseeing the implementation of any post-inspection action plans;

The Director of Legal and Democratic Services is the Senior Responsible Officer with regard to the acquiring of communications data

Central Records

The Council must retain copies of all applications, authorisations, copies of notices and withdrawals of authorisations and cancellation of notices, cross-referenced against each associated document. This will be coordinated by the RIPA Lead Officer, who is currently Trading Standards Manager. When the NAFN system is being used copies of the notices and authorisations are not routinely provided to the Designated Person, but print-offs of the completed online application forms will need to be provided to the Lead Officer. Inspectors from the Interception of Communications Commissioner's Office will be able to obtain copies of all of these documents from NAFN.

The Senior Responsible Officer will have access to all of these forms as and when required.

The Authority must also keep a record of:

- Number of applications rejected by Designated Persons;
- Number of notices requiring disclosure of communications data within the meaning of each subsection of Section 21(4);
- Number of authorisations for acquiring of communications data within the meaning of each subsection of Section 21(4);
- Number of times an urgent notice is given orally (However we do not make use of urgent notices);

The Lead Officer will keep a database of all applications, plus any notices and authorisations whether they are issued by the Authority or issued by NAFN on our behalf. This database will include records of any errors that have occurred. NAFN are able to provide on request statistical information about the numbers of notices or authorisations that they have issued on behalf of the Council during a particular time period

Code of Practice

The Council and those persons acting under of the Act must have regard to the Code of Practice on the Acquisition and Disclosure of Communications Data issued by the Home Office under the Act. Each Designated Person and any other persons involved in the acquisition of communications data will have access to a copy of this code.

Interception of Communications Commissioner's Office

The exercise of the powers and duties relating to communications data is kept under review by inspectors who work for the Interception of Communications Commissioner's Office (IOCCO) under the control of the Interception of Communications Commissioner.

IOCCO state that if we receive a Freedom of Information request for a copy of our inspection report we should notify IOCCO, who will provide us with a suitably redacted version of the report to submit to the requester. No disclosure must take place until IOCCO has been consulted.

Chapter II of Part I of the
Regulation of Investigatory Powers Act 2002 (RIPA)

Reporting of an Error by Accredited SPOC - Form CD5

Name of Public Authority reporting this error: Rhondda Cynon Taff County Borough Council

An error can only occur after a designated person:

- Has granted an authorisation and the acquisition of data ahs been initiated, or
- Has given notice and the notice has been served on a CSP in writing, electronically or orally.

1) Name of Accredited SPOC		**4) SPOC's Telephone Number**	
2) Office, Rank or Position of SpoC		**5) SPOC's Fax Number**	
3) SPOC's Email Address		**6) The error can be reported by email to**	**Ch2.inspectorate@homeoffice.gsi.gov.uk**

7) DETAILS OF THE ERROR
State whether Notice or Authorisation; Notice URN: - **Describe the communications data applied for as set out on the application;** **Describe the nature of the error;** **Date and time the error occurred; Date Time** **If the error was made by the CSP – Name of CSP; and state whether CSP has been informed.** **Yes:** **No: Include reason why CSP not informed:**
8) UNINTENDED COLLATERAL INTRUSION
If any has taken place, please describe what it was;
9) PREVENTION OF SIMILAR ERRORS REOCURRING
What steps have been, or will be, taken to ensure that a similar error does not reoccur
10) REPORTING OF THE ERROR TO THE COMMISSIONER AND NOTIFYING THE SENIOR RESPONSIBLE OFFICER AND THE DESIGNATED PERSON ***Note; there is a requirement to report the error to your senior responsible officer (SRO) and then to the Commissioner***

Details of the SRO	**Name of the SRO Telephone No** **Email address of SRO**
Details of the DP	**Name of the DP Telephone No** **Email address of DP**
The date and time the report has been completed by SpoC	**Date Time**

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: