

## INVESTIGATION OF OFFENCES BY THE COUNCIL - USE OF COVERT SURVEILLANCE

**EXECUTIVE MEMBER:** Councillor Gillian Troughton, Portfolio Holder for Finance and Resources.  
**LEAD OFFICER:** Darienne Law, Head of Corporate Resources.  
**REPORT AUTHOR:** Clinton Boyce, Legal Services Manager.

### WHAT BENEFITS WILL THESE PROPOSALS BRING TO COPELAND RESIDENTS?

The report advises Members of recent changes in the law relating to the use of covert surveillance and seeks approval to the adoption of a revised policy which prescribes how the Council should undertake such surveillance. It also recommends changes to the scheme of delegation in respect of the authorisation of surveillance and advises Members of the outcome of a recent inspection by an Assistant Surveillance Commissioner.

### WHY HAS THIS REPORT COME TO THE EXECUTIVE?

**(eg Key Decision, Policy recommendation for Full Council, at request of Council, etc.)**

The Home Office relevant code of practice on covert surveillance recommends that members review the use of surveillance annually. The report also recommends the adoption of new procedures and changes to the scheme of delegation.

### RECOMMENDATIONS:

- (1) That the changes to the legislative framework, the previous use by the Council of covert surveillance and the Assistant Surveillance Commissioner's report be noted;
- (2) That the draft 'Policy and Procedures Document on the Regulation of Investigatory Powers Act 2000' at Appendix A be approved for use by the Council in respect of dealing with matters relating to covert surveillance;
- (3) That a recommendation be made to Council that the scheme of delegation be amended to reflect that only the following persons are authorised to grant, amend, renew and cancel authorisations: the Chief Executive, the Director of Services, the Head of Corporate Resources, the Democratic Services Manager, the Legal Services Manager and the Waste Services Manager provided that they may only exercise such delegation if they have completed an appropriate training course; and

- |  |
|--|
| (4) That in accordance with the relevant Code of Practice a report be submitted to the Executive on an annual basis reviewing the use of surveillance by the Council in the previous year. |
|--|

## **1. INTRODUCTION**

- 1.1 Council officers investigate many types of offences ranging from benefit fraud, environmental nuisance and breaches of planning law through to dog fouling and littering. If the investigation is carried out without the offender knowing that he is being observed then this amounts to directed covert surveillance. If a Council Officer uses an individual to obtain evidence (e.g. sending someone under the age of 18 into a public house to purchase alcohol) without the potential offender knowing then this would be known as using a covert human intelligence source, commonly known as a 'CHIS'.
- 1.2 Such surveillance is contrary to human rights legislation unless it is carried out in accordance with the law and is necessary and proportionate. The relevant law is the Regulation of Investigatory Powers Act 2000 ('RIPA'). This Act allows covert surveillance to take place where it is necessary for the prevention or detection of crime provided certain safeguards are put in place and the surveillance authorised.
- 1.2 Examples of covert surveillance could be officers placing noise monitoring equipment in an adjacent property or watching a person frequent a property. Enforcement officers carrying out their normal duties and visible would not be covert surveillance.
- 1.4 The Council cannot be law undertake intrusive surveillance which is observing what goes on in a residential property or private car.
- 1.5 Covert surveillance can be carried out by an officer if it is necessary, proportionate, for the purpose of investigating an offence and authorised internally by a designated officer.

## **2. CHANGES IN THE LAW**

- 2.1 From the 1<sup>st</sup> November 2012 two important changes to the law were introduced by the Protection of Freedoms Act 2012.
- 2.2 Firstly, the type of offence for which an authorisation could be granted is restricted to those which carry a sentence of at least 6 months imprisonment or relate to trading offences of selling alcohol or tobacco to children. This significantly reduces the range of offences for which covert surveillance can be

used. Only benefit fraud, food safety and some licensing offences are likely to remain.

- 2.3 Secondly, an authorisation granted by a designated officer must now be approved by magistrate therefore requiring an application to the Court.

### **3. USE BY THE COUNCIL OF AUTHORISED SURVEILLANCE**

- 3.1 The Council has used covert surveillance once in the last three years. Benefit fraud investigations are generally undertaken jointly with the DWP who can provide a dual authorisation for council tax and housing benefit fraud investigations. The reason for this is that most investigations are carried out overtly. In noise nuisance the alleged offender is advised that they are being monitored – this in itself can reduce the level of noise immediately. Food investigations cannot be carried out without the alleged offender knowing. Enforcement officers are visible; even if they are in plain clothes observing a location known for offending this will not constitute covert surveillance as they are merely observing a location and then reacting to any offences which they may observe. The licensing trading offences are likely to be investigated by Trading Standards; other licensing offences are likely to be investigated overtly by officers walking into premises holding unlicensed activities when they are happening.
- 3.2 Despite such low use the Council must have in place procedures for granting authorisations for when they may need to be used. The Council will still be inspected on a three yearly basis by the Surveillance Commissioner.

### **4 SURVEILLANCE COMMISSIONER INSPECTION**

The Council was inspected by an Assistant Surveillance Commissioner on the 16<sup>th</sup> October 2012 and his inspection report is attached at Appendix A. The recommendations set out in that report can be accepted.

### **5 POLICY**

It is necessary to have in place a policy for dealing with the grant, etc of authorisations. A draft policy is attached at Appendix B. This is a detailed document setting out procedures to be followed and forms to be used. The redrafting of the document to take into account the changes of the legislation has allowed it to be considered by the Commissioner. His proposed amendments have been included. Members are asked to approve that document. The Assistant Commissioner recommends that appendix 2 of that policy is merged into the policy itself rather than forming a separate appendix. This will be done prior to issue to staff and will not make any substantive content change.

## **6 SCHEME OF DELEGATION**

- 6.1 In 2010 new legislation designated chief executives, directors, heads of service and service managers as capable of granting authorisations. The scheme of delegation reflected this. The Commissioner has recommended that those authorised be restricted to a smaller number, perhaps three or four in addition to the Chief Executive, adding that those authorised must have received training. So far, the Head of Corporate Resources and the Legal, Democratic and Waste Services Managers have been trained. In practical terms, taking into account likely use, an argument that the authorisation process should have impartiality and those already trained it would be sensible for those capable of authorising requests for covert surveillance to be restricted to the those four officers along with the Director of Services and the Chief Executive the latter being recommended by the Commissioner as being included.
- 6.2 Further training on the Act and recent legislative changes will be arranged for early 2013 for all officers.
- 6.3 No changes are proposed to the officer who is the Senior Responsible Officer for RIPA purposes which is the Democratic Services Manager with his deputy being the Head of Corporate Resources.

## **7. ALTERNATIVE OPTIONS TO BE CONSIDERED**

No other options exist. The procedures are based in statute.

## **8. CONCLUSIONS**

- 8.1 The requirements for a policy, appropriate delegation and three yearly inspections flow from statute or statutory guidance and the Council is required to have procedures in place for dealing with surveillance.
- 8.2 Members are asked to endorse the recommendations as set out above in the box on page 1.

## **9. STATUTORY OFFICER COMMENTS**

- 9.1 The Monitoring Officer's comments are: The legal position is set out above and in Appendix B.

- 9.2 The Section 151 Officer's comments are: No costs arise from this report.
- 9.3 EIA Comments: Neither this report or the attached draft policy at Appendix B have any direct consequences for equality in terms of race, gender, disability, socio-economic, etc. This applies both to the crime threshold for use of directed surveillance by the Council and the judicial approval for such.
- 9.4 Policy Framework: Neither the community strategy or the Council's corporate strategy and policy framework directly relate to this report or the attached draft policy. Revenue and capital budgets do not need to be adjusted as the cost of granting authorisations can continue to be contained within existing staffing resources.
- 9.5 Other consultee comments, if any: None.

**10. HOW WILL THE PROPOSALS BE PROJECT MANAGED AND HOW ARE THE RISKS GOING TO BE MANAGED?**

- 10.1 The proposed delegations and the attached proposed policy set out how the authorisation procedure will be managed.
- 10.2 The internal authorisation of requests to undertake surveillance together with the new requirement for judicial approval will ensure that surveillance is only carried out where it is essential, necessary and proportionate. A risk may arise in respect of collateral intrusion where the privacy of those not the subject of an investigation is affected. The authorisation process should take this into account and consider how such intrusion can be minimised if not removed. A further risk may arise from officers carrying out surveillance without realising that it should have been authorised. This is a matter for training and the training to be provided in early 2013 should be arranged in a manner that all officers directly or indirectly coming into contact with surveillance are trained either through a course or by separate briefings.

**11. WHAT MEASURABLE OUTCOMES OR OUTPUTS WILL ARISE FROM THIS REPORT?**

An established and Commissioner approved framework for dealing with surveillance.

**List of Appendices**

Appendix A: Surveillance Commissioner's inspection report dated 16<sup>th</sup> October 2012;  
and

Appendix B: Draft policy and procedures document on the Regulation of Investigatory Powers Act 2000.

**List of Background Documents:**

Appendices A and B.



Office of Surveillance  
Commissioners

Chief Surveillance Commissioner,  
Office of Surveillance Commissioners,  
PO Box 29105,  
London,  
SW1V 1ZU.

22<sup>nd</sup> October 2012

**COPELAND BOROUGH COUNCIL**

**INSPECTION REPORT**

Inspection date 16<sup>th</sup> October 2012

Inspector Sir David Clarke  
Assistant Surveillance Commissioner

**Introduction**

1. The Council (CBC) serves a population of some 70,000 in a mainly rural coastal area of West Cumbria, from Whitehaven in the north to Millom in the south, including the Sellafield nuclear fuel complex and its surrounding villages.
2. The Senior Corporate Management structure is headed by the Chief Executive, supported by the Director of Services and five Heads of Service.
3. The Chief Executive is Paul Walker, whose address is The Copeland Centre, Catherine Street, Whitehaven, Cumbria CA28 7SJ.
4. The most recent OSC inspection of CBC was conducted by Graham Wright, Surveillance Inspector, on 7<sup>th</sup> May 2009 (report dated 13<sup>th</sup> May).
5. CBC is an infrequent user of RIPA, having granted only one directed surveillance authorisation since the last inspection. It has never made a Covert Human Information Source (CHIS) authorisation.

**Inspection**

6. I carried out the inspection on 16<sup>th</sup> October 2012 at the Copeland Centre. I met the following council officers:
  - Darienne Law, Head of Corporate Resources;
  - Tim Capper, Democratic Services Manager;
  - Clinton Boyce, a solicitor, Legal Services Manager.

7. Mrs Law is a member of CBC's senior management team, reporting directly to the Chief Executive. In 2010 the post of Head of Legal and Democratic Services, held by Mr Jepson at the time of the 2009 inspection, was abolished, and separate Democratic and Legal Services Managers were appointed, both reporting to Mrs Law. Mr Capper, the Democratic Services Manager, succeeded Mr Jepson as CBC's Monitoring Officer.
8. Following the publication of the 2010 RIPA Codes of Practice, Mrs Law was designated to be CBC's Senior Responsible Officer (SRO) for the purposes of RIPA. But in a management restructure in 2012, which gave wider responsibilities to Mrs Law, the role of SRO was transferred to Mr Capper, who also acts as RIPA Coordinator and keeper of the central record of RIPA authorisations. Mrs Law remains an Authorising Officer (AO), and it was she who made the single authorisation in the period under review.
9. Mr Capper is not a member of CBC's senior management board, and to that extent his designation as SRO does not accord with the best practice recommended in paragraph 3.29 of the Covert Surveillance Code. In theory, he is required to exercise oversight over AOs above him in the hierarchy. But having discussed the matter with all three officers, I am satisfied that, in this small local authority with little RIPA activity, no disadvantage is likely to arise. On the rare occasion of a RIPA application being submitted, it is likely to be thoroughly discussed by all three before formal determination by the AO.
10. The inspection started with a discussion, with Mr Capper and Mr Boyce, of CBC's RIPA management, policy and procedures, the designated authorising officers (AOs), training, and the actions taken on the recommendations in the last OSC report. I then inspected the Central Record and the single RIPA authorisation. Finally I met Mrs Law and Mr Capper for a brief feedback discussion before departing the Copeland Centre.
11. I am grateful to all concerned, particularly Mr Capper who made the arrangements, for their helpful cooperation which greatly eased my task.

### **RIPA Structure**

12. The *Guidance to Staff on RIPA – Directed Surveillance and CHIS*, in force in 2009, is to be superseded shortly by a new *Policy and Procedures Document on RIPA 2000* (the *Policy*) being prepared by Mr Boyce. This he is doing on his own initiative, regarding the former *Guidance* as inadequate.
13. The draft incorporates passages reflecting the legislative changes about to come into force on 1<sup>st</sup> November 2012. My inspection took place one day after publication of the Home Office *Guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance*, together with the Magistrates' Courts (RIPA) Rules 2012 (SI 2012/2563), and I was pleased to find that these had already been printed out for dissemination to applicants and AOs. Some changes to the draft *Policy* will be made in the light of this material.

14. The new draft *Policy* is clear and comprehensive, and in its final form will be a marked advance on the earlier *Guidance* document. I made, however, a number of suggestions for further improvement, the principal points being:

- A clearer distinction between the processes of *review* and *renewal*, with *review* preceding *renewal*;
- The removal of the two passing references<sup>1</sup> to *accessing communications data*, which is a separate topic, governed by the Acquisition and Disclosure of Communications Data Code of Practice and the IOCCO inspection regime and is outside the scope of Part II of RIPA;
- Some revision to paragraph 3.4(b), which deals with the circumstances in which a public volunteer of information may be a CHIS. Though it is unlikely that CBC will ever make a CHIS authorisation, the *Policy* needs to draw attention to the risk that an informant may in reality be a CHIS even if not tasked to obtain information covertly. This is highlighted in paragraph 2.22 of the CHIS Code of Practice. When an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship, alarm bells should begin to ring. It probably means that the informant is in reality a CHIS, to whom a duty of care is owed if the information is then used. This needs to be made clear in the *Policy*, with an exhortation to refer any such instance for legal advice before acting on the information received from such an informant.

**See recommendation**

15. To meet a recommendation of the 2009 inspection that the then *Policy* should include clearer practical guidance on the completion of RIPA forms, a separate guidance document was annexed as an Appendix to the *Policy*. This is a good practical guide and will now be incorporated into the *Policy* as part of a single integrated corporate policy and guidance document.

16. The former *Policy* provided that RIPA authorisations could be made by all members of the Corporate Team, or by the Chief Legal Officer in that person's absence. The new draft *Policy* identifies the Chief Executive, Director of Services and the five Heads of Service as AOs, but then adds "*Any Service Manager reporting directly to a Head of Service*".

17. Mr Boyce explained to me that this designation was made in conformity with SI 2010/521, which specifies *Service Manager or equivalent* as the minimum level of AO for the purposes of a directed surveillance or CHIS authorisation. There are some 12-15 such Service Managers, but no composite list of them is maintained, and in discussion it was clear that many of them would never in practice be called upon to act as a RIPA AO. Bearing in mind that nobody should be an AO unless trained for that role, CBC should consider designating

---

<sup>1</sup> These are at paragraphs 4.3.6 and 4.6/4.6.1 in the present draft *Policy*

a much smaller number of AOs, say three or four in addition to the Chief Executive, all being persons who have attended the appropriate AO training.

**See recommendation**

18. The Central Record, as reported by Mr Wright, is a computer spreadsheet containing the information now set out in paragraph 8.1 of the Covert Surveillance Code. The single authorisation in the period under review was made in relation to a benefit fraud investigation. I enquired into other aspects of CBC's enforcement activities which might give rise to RIPA usage.
19. CBC has not been involved in any antisocial behaviour investigation for some years. It has no covert camera equipment for use in fly-tipping or dog fouling investigations or the like. Licensing enforcement is carried out overtly. CBC is conscious of the forthcoming imprisonable crime threshold and recognises that RIPA usage will continue to be a rare event, though there may be continuing usage in benefit fraud investigations in the light of DWP's recent decision to restrict directed surveillance authorisations to cases which cross a higher financial threshold. I was told that during the period under review, CBC investigators participated in a number of surveillance operations conducted jointly with DWP, under DWP authorisations.
20. I drew attention to paragraph 3.30 of the Covert Surveillance Code, suggesting regular reports to the elected members, a practice which Mr Capper will henceforth adopt.

**Training**

21. A programme of periodic RIPA training is maintained. A training day was held in March 2012 for AOs and some applicants, the training being delivered by ITS Training (UK) Ltd. No bespoke attendance record was made, but Mr Capper was able to show me emails confirming the attendance list.
22. It was clear that not all potential AOs attended the course, nor all potential RIPA applicants. It is proposed to hold refresher training shortly, to update staff on the new legislative changes coming into force, and to arrange a full annual refresher in early 2013. An accurate and accessible attendance record will be established and maintained in the future; no formal recommendation is required.

**Examination of documents**

23. I examined the single RIPA authorisation, made in June 2012 in a "living together" benefit fraud investigation. This was well articulated by the applicant, with full details of the proposed surveillance, its necessity and proportionality, and good consideration of the issues of collateral intrusion. The surveillance was to be carried out jointly with the DWP, since income support was also in payment.
24. Unfortunately the AO did not complete the "5 W's" box, and only expressed very brief conclusions on necessity and proportionality; this might have made the authorisation vulnerable to challenge.

25. The expiry date was set a day too late (failing to deduct one day from the full three month period), and the AO purported to set a review on the day of expiry. In due course a proper cancellation was effected, recording that sufficient evidence of living together had been obtained during the 12 weeks so as to justify further action.
26. I discussed these findings with the AO, Mrs Law. I suggested that reviews should preferably have been set at monthly intervals, so that the necessity and proportionality of continued surveillance could be formally considered periodically as time went by. She explained that though no formal review forms were completed, she regularly discussed the progress of the surveillance with the investigator (applicant). The surveillance only bore fruit in the latter part of the three month period. Ideally, and to render the surveillance less vulnerable to challenge, these decisions should have been formalised and recorded as reviews.

**See recommendation**

## **CCTV**

27. The Council's town centre CCTV system is located in the police station and is monitored (if at all) by police officers, under an agreement with Cumbria Police. I was told that no CCTV operators are employed by CBC. Accordingly, any covert use by the police of the overt CCTV system must be covered by RIPA authorisations made by the police, in which CBC does not become involved.

## **Conclusions**

28. In a small authority making very infrequent use of its RIPA powers, I was impressed by the steps taken to maintain a compliant RIPA structure, particularly the work done on the new *Policy*, and to maintain a programme of regular training. My visit was timely, shortly before the final drafting of the *Policy* and the implementation of the forthcoming legislative changes.
29. It was disappointing to find some deficiencies in the one authorisation, but the AO and SRO readily accepted my observations and I have no doubt that they will heed them when dealing with any future RIPA authorisations, rare though these occasions might be.

30. Accordingly I make the following

## **Recommendations**

- I. *That the draft Policy be revised in accordance with paragraph 14 of this report, before being formally adopted by the Council;*
- II. *That CBC designate a smaller number of officers as RIPA authorising officers, a record of their RIPA training being maintained;*

*III. That in making authorisations in future, the authorising officer sets and holds timely reviews, at which the continued necessity and proportionality of the authorised covert activity is formally considered and recorded.*

**David Clarke**  
**Assistant Surveillance Commissioner**



*Proud of our past. Energised for our future.*

**DRAFT**

**POLICY AND PROCEDURES**

**DOCUMENT**

**ON**

**THE REGULATION OF**

**INVESTIGATORY POWERS ACT**

**2000**

Draft revision 1 date: 4<sup>th</sup> October 2012

Draft revision 2 date: 22<sup>nd</sup> November 2012

Draft approved:

Next revision due: 1<sup>st</sup> December 2013

## INDEX

	Page
1. Introduction	4
2. Covert Surveillance	7
2.1 Introduction	7
2.2 Meaning of surveillance	7
2.3 Meaning of covert surveillance	7
2.4 Meaning of intrusive surveillance	7
2.5 Meaning of directed surveillance	8
2.6 Limitation on the use of directed covert surveillance	8
2.7 Meaning of private information	9
2.8 Tracking devices	10
2.9 Exceptions where a RIPA authorisation is not required	10
2.10 CCTV and ANPR systems	10
2.11 Use of noise monitoring equipment	11
2.12 Example of the use of directed surveillance	11
2.13 Grounds for making an authorisation under RIPA	11
2.14 Core functions	12
2.15 Further guidance of covert surveillance	12
3. The Conduct of Covert Human Intelligence Sources	13
3.1 Grounds for granting authorisation	13
3.2 Meaning of CHIS	13
3.3 Meaning of relationship	13
3.4 Examples where the use of CHIS may arise	14
3.5 Further guidance on the use of CHIS	15
4. The Procedure for Obtaining Authorisations (Directed Surveillance and CHIS)	16
4.1 Introduction	16
4.2 Authorising officers	16
4.3 Making an application for an authorisation	16
4.4 Urgent cases	21
4.5 Specific matters relating to CHIS	21
4.6 Specific matters relating to accessing communications data	23
4.7 Obtaining judicial approval of authorisations	23
4.8 Cases where authorisations must be obtained from specifically designated officers	24
4.9 Duration, review and cancellation of authorisations	25
4.10 Maintaining records of authorisations, renewals and	27

cancellations

5.	General	28
5.1	The Senior Responsible Officer	28
5.2	Chief Surveillance Commissioner	28
5.3	Officer training	28

## APPENDIX 1

Application forms for:

Authorisation Directed Surveillance  
Renewal of a Directed Surveillance Authorisation  
Review of a Directed Surveillance Authorisation  
Cancellation of a Directed Surveillance Authorisation  
Authorisation of the conduct or use of a Covert Human Intelligence source (CHIS)  
Renewal of a Covert Human Intelligence (CHIS) Authorisation  
Review of a Covert Human Intelligence Source (CHIS) Authorisation  
Cancellation of an authorisation for the use or conduct of a Covert Human Intelligence Source

## APPENDIX 2

Additional guidance on completion of forms.

# **1. Introduction**

- 1.1 The Regulation of Investigatory Powers Act 2000 ('RIPA') and regulations, orders and codes of practice made under RIPA create a framework for the regulation of covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that the UK's law enforcement and security agencies have the powers they need to do their job effectively.
- 1.2 An individual's rights relate to privacy and are contained in human rights legislation, both European and national. They introduce a remedy for persons claiming that their privacy has been breached. It is not an absolute right however. The right will not apply if the interference with a person's privacy is in accordance with the law, necessary and proportionate. This exception to the right has been incorporated into English law by the enactment of part II of RIPA.
- 1.3 The Council intends to use RIPA sparingly and only in extreme cases. It believes in overt investigatory operations and keeping interferences with a person's privacy to an absolute minimum. This is reflected in the low number of authorisations granted over recent years.
- 1.4 If an investigation is carried out in accordance with RIPA procedures, then any possible resultant breach of a person's privacy rights would not be actionable as a civil claim. In addition, in criminal proceedings arising from the investigation, the evidence gathered will not be challengeable under Section 78 of the Police and Criminal Evidence Act 1984, on the ground that it is a breach of privacy rights. The protection afforded by RIPA also extends to complaints made to the Investigatory Powers Tribunal and to the local government ombudsman. Strict adherence to the requirements of RIPA therefore provides a defence to any civil proceedings and claims for damages for breach of privacy.
- 1.5 It is therefore crucial that all investigating officers adhere to the requirements of RIPA.
- 1.6 The purpose of this guidance is to:
  - (a) explain the scope of the relevant parts of RIPA and the circumstances where it applies;
  - (b) provide guidance and give advice to those services undertaking covert surveillance and on the authorisation procedures to be followed in respect of authorisations, renewals and cancellations; and
  - (c) ensure full compliance with RIPA and a Council-wide consistent approach to its interpretation and application.

- 1.7 The Council has had regard to the Home Office Code of Practice on Covert Surveillance and Property Interference (2010) and the Code of Practice on Covert Human Intelligence Sources (2010) and each department has copies to which staff can refer.

In the electronic form of this document the Codes are available by pressing 'Ctrl' and clicking on following these links:

Covert Surveillance and Property Interference:

[www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary](http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary)

Covert Human Intelligence Sources:

[www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-human-intel?view=Binary](http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-human-intel?view=Binary)

- 1.8 In summary RIPA requires that when the Council undertakes directed surveillance or uses a Covert Human Intelligence Source ("CHIS") these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied.
- 1.9 Surveillance operations authorisations can be made by a Director, Head of Service or Service Manager or equivalent as permitted by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (S.I. 2010 No. 521). That Order restricts the power to grant authorisations for the purpose of preventing or detecting crime or of preventing disorder. However only those officers who are trained can authorise surveillance and guidance, particularly that of the Surveillance Commissioner, recommends that only the Chief Executive and a small number of officers be allowed to authorise surveillance. Only the following persons are therefore authorised to grant authorisations:
- Chief Executive;  
Director of Services;  
Head of Corporate Resources;  
Democratic Services Manager;  
Legal Services Manager; and  
Waste Services Manager.
- 1.10 The Senior Responsible Officer ('SRO') for RIPA purposes is the Council's Democratic Services Manager. The Head of Corporate Resources is his deputy.
- 1.11 From the 1<sup>st</sup> November 2012 two important changes are made to RIPA authorisations:
- (a) the person authorising directed surveillance for the purpose of preventing or detecting crime or of preventing disorder can only do so if two conditions are met. The first is that the conduct being prevented or

detected constitutes one or more criminal offences or corresponds to conduct which would constitute one or more criminal offences. The second condition is that the criminal offence is punishable by a maximum term of at least 6 months imprisonment or is an offence under section 146 (sale of alcohol to children), section 147 (allowing the sale of alcohol to children) or section 147A (persistently selling alcohol to children) of the Licensing Act 2003 or is an offence under section 7 of the Children and Young Persons Act 1933 (sale of tobacco, etc to persons under the age of 18). This is an important changes as it means that authorisations cannot be granted for minor offences particularly those where fixed penalty notices could be issued. This change is made by the Regulation of Investigatory Powers (Directed surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (S.I. 2012 No. 1500). This is considered further in paragraph 2.6; and

- (b) whilst an officer listed above can grant an authorisation section 38 of the Protection of Freedoms Act 2012 introduces a new section 32A and 32B to RIPA. These new sections require authorisations for directed surveillance under section 28 of RIPA and authorisations for covert human intelligence sources under section 29 of RIPA to be approved by the 'relevant judicial authority' before the authorisation can take effect. The judicial authority is a justice of the peace. This matter is dealt with further below at paragraph

- 1.12 It should be noted that the Council cannot authorise "intrusive surveillance". Such surveillance is, by section 26(3) of RIPA, covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicles and involves the presence of an individual on the premises or in the vehicles or is carried out by means of a surveillance device. If the device is designed or has the main purpose of providing information about the location of the vehicle then this will not be intrusive.
- 1.13 No Council Officer can authorise interference or interception with any communication in the course of its transmission by the public postal service or public telecommunications system. Part I of RIPA deals with interception of communications and the acquisition and disclosure of communications data.
- 1.14 The SRO will maintain centralised records of all authorisations for covert surveillance or CHIS and monitor them to ensure uniformity of practice. The central records shall contain information regarding reviews, renewals and cancellations. Original authorisations is for each service unit to retain its authorisations on a centralised file, and for a copy to be put on the individual case file.

## **2. Covert Surveillance**

### **2.1 *Introduction***

RIPA provides for the authorisation of covert surveillance by public authorities, where the surveillance is likely to result in the obtaining of private information about a person. It does so by establishing a procedure for authorising covert surveillance. It prescribes the office, rank and position of those permitted to authorise covert surveillance. From 1<sup>st</sup> November 2012 the authorisation process will be subject to judicial approval and any authorisation granted by a local authority will not take effect unless it is approved by the Magistrates' Court.

### **2.2 *Meaning of 'surveillance'***

Surveillance includes:-

- (a) monitoring, observing or listening to persons their movements, their conversations or any of their activities or communications;
- (b) recording anything monitored, observed or listened to in the course of surveillance; and
- (c) surveillance by or with the assistance of any surveillance device.

### **2.3 *Meaning of 'covert surveillance'***

Covert Surveillance is any surveillance which is carried out in a manner calculated to ensure that the subject is unaware it is, or may be taking place. The provisions of RIPA authorise the following forms of covert surveillance:

- (a) directed surveillance;
- (b) intrusive surveillance; and
- (c) the conduct and use of covert human intelligence sources ('CHIS').

### **2.4 *Meaning of 'intrusive surveillance'***

**Note that RIPA does not enable a local authority to make any authorisations to carry out intrusive surveillance.**

Intrusive Surveillance is surveillance which is covert surveillance that:

- (a) is carried out in relation to anything taking place in any residential premises or any private vehicle; and
- (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

Residential premises include a rental flat occupied for residential purposes, a

police cell and a hotel bedroom.

Examples of places which may **not** be regarded as residential premises are a communal stairway in a block of flats or the front garden of premises readily visible to the public.

There are a number of exceptions applicable to the use of certain monitoring equipment some of which are not considered to constitute the use of intrusive surveillance. It is important to note that not all surveillance of a suspect's home or vehicle is likely to amount to intrusive surveillance. For example, if an Investigating Officer observes a suspect leaving his home from the street using binoculars, this is unlikely to be intrusive, unless the quality of the image obtained is of the same quality as might be expected to be obtained from a device actually present on the premises. But the intrusiveness of the surveillance proposed must be considered before any surveillance operation takes place.

For the avoidance of doubt, surveillance that enables an Investigating Officer to view or monitor anything going on inside a dwelling is almost certainly going to be regarded as intrusive and conduct of that nature cannot be authorised by a local authority.

## **2.5 *Meaning of 'directed surveillance'***

Local authorities are permitted under RIPA to authorise directed covert surveillance on the grounds that such surveillance is necessary for the prevention or detection of crime . Surveillance is directed if it is covert but not intrusive and is undertaken:

- (a) for the purpose of a specific investigation or a specific operation;
- (b) in such a manner as is likely to result in the obtaining of private information (see 2.7 below) about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- (c) otherwise and by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

## **2.6 *Limitation on the Use of Directed Covert Surveillance***

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI 2012/1500) (2012 Order) will come into force on 1 November 2012. It restricts Authorising Officers in a local authority in England or Wales, from authorising the carrying out of directed surveillance unless it is for the purpose of preventing or detecting a criminal offence and meets the following conditions:

- (a) that the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment or
- (b) constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

It is therefore essential that Investigating officers consider the penalty attached to the criminal offence which they are investigating, before considering whether it may be possible to obtain an authorisation for directed surveillance.

## 2.7 ***Meaning of 'private information'***

Information is considered to be private information if it includes any information relating to the subject's private or family life or the private or family life of any other person. It would include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Private information may include personal data for example names, telephone numbers and address details.

Private information may be acquired through covert surveillance even where a person is in a public place and may have a reduced expectation of privacy. For example, where two people hold a conversation on the street they may have a reasonable expectation of privacy over the contents of that conversation. A directed surveillance authorisation may therefore be required if a public authority records or listens to the conversation as part of a specific investigation or operation.

Note also that the information relating to the private life of an individual may be obtained when a number of records are analysed together, or where a number of pieces of information are obtained, covertly, for the purpose of making a record about a person or for data processing to generate further information. The totality of the information may constitute private information even if the individual records do not.

For example, enforcement officers may photograph the exterior of business premises for record purposes without the need for a RIPA authorisation. If, however the officers wished to establish a pattern of occupancy of those premises by any person and took photographs on a number of occasions, that conduct would be likely to result in the obtaining of private information and a RIPA authorisation would be needed.

## 2.8 *Tracking devices*

The use of a surveillance device designed or adapted for the purpose of providing information regarding the location of a vehicle does not necessarily constitute directed surveillance as it may not provide private information about any individual, but simply information about the location of the device at any one time. However, using that information coupled with other surveillance activity which may obtain private information, may amount to directed surveillance and an authorisation may be required.

## 2.9 *Exceptions where a RIPA Authorisation is not required*

Some surveillance activity does not constitute directed surveillance for the purposes of RIPA and no authorisation can be provided for such activity. These activities include:

- (a) covert surveillance by way of an immediate response to events;
- (b) covert surveillance as part of general observation activities -for example, if enforcement officers attend a market where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of any particular individual and their intention is to identify and tackle offenders, then this forms part of the general duties of the public authority and the obtaining of private information is unlikely. In such a case a directed surveillance authorisation need not be sought;
- (c) covert surveillance not relating to the prevention or detection of crime or the prevention of disorder; and
- (d) overt surveillance by CCTV and automatic number plate recognition (APNR) systems.

## 2.10 *CCTV and ANPR Systems*

Where overt surveillance equipment is used for example in town centres, members of the public will be aware of the use and no RIPA authorisation is required. The use of an ANPR system to monitor traffic flows or to detect traffic offences would not require a RIPA authorisation.

If, however, CCTV cameras or an ANPR system are used in a covert, pre-planned manner as part of a specific investigation or operation for the surveillance of a particular individual, then an authorisation for directed surveillance may be required. Such surveillance is likely to result in the obtaining of private information about a person, that is, a record of his movements and activities.

Part 2 (sections 29 to 36) of the Protection of Freedoms Act 2012 intends to regulate CCTV and other surveillance camera technology. These provisions require the Secretary of State to issue a code of practice on the use of such system. It is understood that a draft code will be issued in autumn 2012 with

the aim of bringing it into force in April 2013. The Council will be required to have regard to the code when exercising functions which the code will relate to. This policy will be updated once the code is in force.

#### 2.11 *Use of Noise Monitoring Equipment*

Where possible the use of noise monitoring equipment should be notified to the owner and occupier of the offending premises. Where this is not possible, covert monitoring may be considered a reasonable and proportionate approach. If it is decided to seek an authorisation, then the Authorising Officer should consider whether the surveillance equipment is capable of measuring volume only, or whether it can identify individuals, being mindful that the more sensitive the equipment, the greater the risk that the surveillance will be Intrusive Surveillance.

If the noise monitoring equipment is calibrated only to detect excessive noise levels it may be considered that no private information is likely to be obtained and it may be that in such circumstances, an authorisation is not necessary.

#### 2.12 *An Example of the Use of Directed Surveillance*

This type of surveillance may be used to gather evidence for an offence such as a fraudulent claim for housing benefit. An Investigating Officer may need to carry out surveillance of a suspect's home to obtain information about their contacts and work patterns. This would be directed surveillance as it would result in obtaining private information. A RIPA authorisation should be obtained. The Investigating Officer would need to demonstrate that such surveillance was necessary and proportionate. The Authorising Officer must be satisfied that the action proposed would not amount to intrusive surveillance and place conditions on the conduct to avoid this happening prior to authorising the application or decline to authorise as necessary.

Note that if the surveillance involves the use of a surveillance device, that provides detail of the same quality as may be expected to be obtained by a device located on the premises, this may amount to intrusive surveillance. No RIPA authorisation may be given for intrusive surveillance.

#### 2.13 *Grounds for Making an Authorisation under RIPA*

The grounds on which a local authority may make an authorisation permitting the use of directed surveillance under RIPA are **limited to the prevention or detection of crime or the prevention of disorder**. If directed surveillance is carried out for any other purpose, then an authorisation under RIPA cannot be granted.

#### 2.14 ***Core Functions***

A local authority may only make authorisations under RIPA when performing its core functions. Those are the specific public functions undertaken by the local authority as opposed to its ordinary functions which are undertaken by all public authorities.

For example, an authorisation under RIPA cannot be used when the principal purpose of an investigation is for taking disciplinary action against an employee, as the disciplining of an employee is not a core function. It may, however, be appropriate to seek an authorisation under RIPA if there are associated criminal investigations.

#### 2.15 ***Further Guidance on Covert Surveillance***

Further guidance on the use of covert surveillance may be found in the Home Office Code of Practice for Covert Surveillance and Property Interference at the link shown in paragraph 1.6 above.

### **3. The Conduct of Covert Human Intelligence Sources**

#### **3.1 *Grounds for granting authorisation***

A local authority may grant an authorisation under RIPA for the use of a covert human intelligence source (a "CHIS".) The conduct that may be authorised is any conduct that:

- (a) is comprised in any such activity including the conduct of CHIS or use of CHIS, as are specified in the authorisation;
- (b) consists in conduct by or in relation to a person who is so specified or described as a person as to whose actions as a CHIS the authorisation relates;
- (c) is carried out for the purposes of or in connection with the investigation or operation so specified or described;
- (d) is necessary and proportionate to the intelligence dividend that it seeks to achieve;
- (e) is necessary for the purpose of the prevention or detection of crime or the prevention of disorder.

#### **3.2. *Meaning of 'CHIS'***

A person is considered to be a CHIS if:

- (a) s/he establishes or maintains a personal or other relationship with a person for the covert purpose of doing anything falling within paragraphs (b) or (c) below;
- (b) s/he covertly uses such a relationship to obtain information or provide access to any information to another person;
- (c) s/he covertly discloses information obtained by the use of the said relationship, or as a consequence of the existence of such a relationship.

#### **3.3 *Meaning of 'relationship'***

Authorisations for the use of a CHIS do not relate solely to the obtaining of private information. An authorisation is necessary where there is covert manipulation of a relationship to gain any information. Article 8 of ECHR includes the right to establish and develop a relationship so such a right may be infringed where a public authority manipulates that relationship to obtain information.

To establish a relationship simply means to "set up" a relationship and does not require endurance of a relationship over a period of time. The use of a CHIS is most likely to arise when individuals are used to make test purchases. Whether a relationship exists between the buyer and seller depends upon the circumstances, but a repetition of purchases is not always necessary to give rise to a relationship.

### 3.4 *Examples where the use of a CHIS may arise*

- (a) Test purchases – this kind of investigation is commonly undertaken by County Council Trading Standards Officers when carrying out test purchases in off licences. Enforcement Officers of this Council may be drawn into such operations as the Council is licensing authority under the Licensing Act 2003. Council officers should not take part in the investigation relating to test purchases. If offences do arise using evidence from test purchase the correct course of action should then be for Trading Standards to commence a review of the off licence's premises licence. If the Enforcement Officer, as part of that joint investigation, observes Licensing Act offences being committed these are likely to fall as part of his general duties and not constitute covert surveillance.

Test purchases can arise however in respect of taxi fares where a CHIS may be used to hire a taxi to determine if the correct fare is being charged. Such an offence however is unlikely to be one which carries a sentence of imprisonment not less than six months unless there is a pattern of deliberate dishonesty or theft involved.

- (b) Public Volunteers - not every human intelligence source will be a CHIS. Where a person volunteers information to the local authority without being induced, asked or tasked by the local authority, no authorisation under RIPA is required. For example, if a person provides a piece of information about something he has witnessed in his neighbourhood, he would not be regarded as a CHIS as the information he is passing is not as a result of a relationship which has been established or maintained for a covert purpose.

However care needs to be taken with such volunteers. There is a risk that an informant may in reality be a CHIS even if he is not tasked to obtain the information covertly. It is possible that a person could become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. Where an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship then this is likely to mean that the informant is in reality a CHIS to whom a duty of care is owed if the information is then used. Where information is volunteered, more than once, legal advice should be sought before using the information provided by the informant. Paragraphs 2.20 to 2.22 of the Code relating to CHIS provides further information.

For a further example, if a member of the public is asked by an Investigating Officer to maintain a record of vehicles arriving at and leaving a specific location, no relationship has been established or maintained in order to gather that information. A CHIS authorisation is therefore not required. Note there may, in such circumstances, be the need to obtain a RIPA authorisation for directed surveillance.

In contrast, if an Investigating Officer wishes to use a neighbour to question an individual about the activities carried on at a site which for example, was subject to enforcement action under the Planning Acts, this may amount to the use of a covert human intelligence source.

- (c) Professional or Statutory Duty - any regulatory or professional disclosure made by an individual should not result in that individual falling within the definition of a CHIS, as the information disclosed is derived from a business relationship which will not have been established for the covert purpose of disclosing such information. In addition, such disclosure is undertaken as a statutory requirement and is unlikely to infringe an individual's privacy.

### **3.5 Further Guidance on the Use of a CHIS**

Further guidance on the use of a CHIS may be found in the Home Office Covert Human intelligence Sources Code of Practice which can be found at the link shown in paragraph 1.6 above.

## **4. The Procedure for Obtaining Authorisations (Directed Surveillance and CHIS)**

### **4.1 Introduction**

Each form of covert surveillance which is subject to the provisions of RIPA must be authorised in accordance with the provisions of RIPA.

### **4.2 Authorising officers**

Regulations prescribe that within a local authority, Authorising Officers must hold the rank of Director, Head of Service, Service Manager or equivalent. The Council's Scheme of Delegation delegates the Director of Services, all Heads of Service and all Service Managers as Authorising Officers.

No person designated as an Authorising Officer should act as an Authorising Officer unless s/he has undertaken appropriate training within 3 years prior to the date of making an authorisation.

### **4.3 Making an application for an authorisation**

4.3.1 The whole of this section applies to directed surveillance and the use of a CHIS. When completing an application for directed surveillance or use of a CHIS, and when completing review, renewal and cancellation forms, regard should be had to this Policy and Procedure.

4.3.2 The Investigating Officer must complete all of the information required by the appropriate prescribed form. There are different forms for authorising directed surveillance and for authorising the use of CHIS.

Electronically, the forms may be found on the Home Office web site at <http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/>.

The following forms can also be found in Appendix 1 to this document:

1. Application for and authorisation of directed surveillance;
2. Renewal of a directed surveillance authorisation;
3. Review of a directed surveillance authorisation;
4. Cancellation of a directed surveillance authorisation;
5. Application for authorisation of the conduct or use of CHIS;
6. Application for renewal of a CHIS authorisation;

7. Review of a CHIS authorisation; and
8. Cancellation of a CHIS authorisation.

4.3.3 The application form should specify:

- (1) names (where known) or descriptions of the subjects and any known history and character thereof;
- (2) location of the subject and/or surveillance and (if relevant) the place where CHIS is to be located;
- (3) the type of surveillance device or equipment to be used;
- (4) the type of activities, numbers and names of officers who will be the CHISs (if relevant);
- (5) that the surveillance is necessary for the purpose of preventing or detecting crime or of preventing disorder;
- (6) that it is proportionate i.e. specifying:
  - (a) the objectives of the surveillance, the use of a CHIS or the accessing of communications data;
  - (b) the crime or wrong-being investigated (indicate the type of breach);
  - (c) why surveillance, the use of a CHIS or the accessing of communications data should be used in preference to other methods of investigation, for example it may be that it would be a means of obtaining the best evidence or the evidence could be obtained more quickly by surveillance, the use of a CHIS or the accessing of communications data than by other means;
  - (d) why it would be more practicable;

See paragraph 4.3.4 for more information on the meaning of necessary and proportionate.

- (7) the objectives of the activities;
- (8) the name and nature of the investigation or operation and what makes the Authorising Officer believe surveillance, the use of a CHIS or the accessing of communications data will achieve the objectives referred to;
- (9) the length of time which should be proportionate to the wrong being investigated;

- (10) the risk of information relating to third parties' private and family life being obtained. This is known as 'collateral intrusion'; and
- (11) the likelihood of acquiring any confidential/religious material.
- (12) Authorisations should cover all known or reasonably foreseeable eventualities. Accordingly if a subject is likely to move the authorisation should specify this. If a subject is accompanied by, or living with, another person then the authorisation should include that other person if necessary.

Appendix 2 to this Policy and Guidance provides further information on how the forms should be completed.

- 4.3.4 The activities to be authorised must be necessary for the purpose of preventing or detecting crime or of preventing disorder. If they are necessary they must be proportionate to what is sought to be achieved by carrying them out. Both the investigating officer and the authorised officer must balance the seriousness of the intrusion into a person's privacy against the need of undertaking the activity in investigative and operational terms.

The Home Office Code of Practice on covert Surveillance and Property Interference at pages 25 to 27 provide useful information and examples on the necessary and proportionality test. Paragraphs 3.5 and 3.6 are repeated here:

*"3.5 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by less intrusive means.*

*3.6 The following elements of proportionality should therefore be considered:*

- *balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;*
- *explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
- *considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
- *evidencing as far as reasonably practicable, what other methods had been considered and why they were not implemented."*

4.3.5 Authorisations or renewals of authorisations must be given by the Authorising Officer in writing except in urgent cases when it can be done orally. The Authorising Officer should forward a scanned copy of the hand signed authorisation by email immediately to the Senior Responsible Officer (or in his absence the Legal Services Manager). The Senior Responsible Officer (or Legal Services Manager as appropriate) will inform the Authorising Officer of the unique reference number (URN) that has been allocated to that authorisation. The URN must be included on all future review, renewal or cancellation forms in relation to that authorisation.

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

- (a) it is necessary for the purpose of preventing or detecting crime or of preventing disorder. The written authorisation should specify the objectives of the activity in factual terms, for example, to gather evidence. The type of crime must also be specified and what facts led the Authorising Officer to believe that the activity will achieve its objectives;
- (b) it is proportionate to the seriousness of the crime or the matter being investigated and the history and character of the subject concerned.
- (c) the Investigating Officer has completed all relevant sections of the appropriate authorisation form. S/He must also be satisfied that all of the matters detailed in the paragraph headed "Making an Application", above, have been properly considered and set out in sufficient detail on the form.
- (d) that the surveillance proposed may infringe the human rights of its subject or of others. S/He must also be satisfied that the covert surveillance for which the authorisation is sought is proportionate i.e. that the information could not be obtained by any other means and that it is necessary to further the objectives of the investigation. S/He should consider whether the benefits of obtaining the information are significant rather than marginal. S/He must also consider the risk of collateral intrusion into the privacy of other persons.
- (e) In addition when an authorisation is sought for use of CHIS, the Authorising Officer must be satisfied that:
  - (1) there is a person within the investigating team who will have day to day responsibility for dealing with the source on behalf of the authority and that he will ensure the sources security and welfare;

- (2) there will at all times be another person within the investigating team who will have general oversight of the use made of the source;
- (3) there will be a person within the investigating team who will have responsibility for maintaining a record of the use made of the source;
- (4) the records relating to the source contain all matters as may be specified in regulations;
- (5) records maintained that disclose the identity of the source will not be available to persons except to the extent that there is a need for them to be made available; and
- (6) that the form specifies the person to whose actions as a CHIS the authorisation relates, describes the purposes of the investigation or operation and any limit on the conduct authorised.

If the Authorising Officer is not completely satisfied that the form has been properly completed, s/he should liaise with the Investigating Officer to obtain further information.

4.3.7 In considering whether to grant an authorisation the Authorising Officer must demonstrate how s/he has reached the conclusion that the activity is proportionate to what it seeks to achieve. There are four elements of proportionality to consider:

- (a) balancing the size and scope of the operation against the gravity and extent of the perceived crime or offence;
- (b) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- (c) that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and
- (d) evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.

4.3.8 In granting an authorisation the Authorising Officer should clearly set out what activity and surveillance equipment is authorised so that the investigating Officer is certain what has been sanctioned.

#### 4.4 *Urgent cases*

An authorisation may be granted or reviewed orally in any urgent case. The reasons for the urgency must be given and recorded.

#### 4.5 *Specific matters relating to CHIS*

In respect of Covert Human Intelligence Sources in addition to the above it is necessary under S29(5) RIPA that there are in force such arrangements as are necessary for ensuring:

- (a) that there will at all times be a person holding an office, rank or position with the relevant investigatory authority who will have day to day responsibility for dealing with the CHIS on behalf of that authority and for the CHIS's security and welfare;
- (b) that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the CHIS;
- (c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the CHIS;
- (d) that the records relating to the CHIS that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State; and
- (e) that the records maintained by the relevant investigating authority that disclose the identity of the CHIS will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

In other words there must be an officer given direct day to day management of the CHIS to look after his/her needs and another officer in overall control of the use of the CHIS. A record must be made by a specified person of the use of the CHIS. Regulations have been made giving details of the type of particulars needed to be recorded. (See 12 below for details). The identity of CHIS's is not to be disclosed unless there is a need to do so. NB - There is no need for 3 different officers. The person responsible for maintaining a record should be an authorising officer.

- (f) Records relating to the CHIS must contain the following by reason of the Regulation of Investigatory Powers (Source Records) Regulations 2000:-
  - (i) the identity of the CHIS;
  - (ii) the identity, where known, used by the CHIS (ie his or her 'alias');

- (iii) any relevant investigating authority other than the authority maintaining the records;
  - (iv) the means by which the CHIS is referred to within each relevant investigating authority (ie his or her 'code name');
  - (v) any other significant information connected with the security and welfare of the CHIS;
  - (vi) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a CHIS that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the CHIS(s) have where appropriate been properly explained to and understood by the CHIS(s);
  - (vii) the date when, and the circumstances in which, the CHIS was recruited; (or if already employed by WBC and allocated this task);
  - (viii) the identities of the authorising officer and the applicant;
  - (ix) the periods during which those persons have discharged those responsibilities;
  - (x) the tasks given to the CHIS and the demands made of him or her in relation to their activities as a CHIS;
  - (xi) all contacts or communications between the CHIS and a person acting on behalf of any relevant investigating authority;
  - (xii) the information obtained by each relevant investigating authority by the conduct and use of the CHIS;
  - (xiii) any dissemination by that authority of information obtained in that way; and
  - (xiv) in the case of a CHIS who is not an under-cover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the CHIS activities for the benefit of that or any other investigating authority.
- Therefore, the officer in charge of maintaining a record of the use of each CHIS should record all these details. The way these records are kept is designed to try to keep the CHIS safe from discovery by the subjects and safe from any harm which could result from their disclosure and also to keep in the open any money or other benefits paid to a CHIS who is not an employee officer of an authorising body.

Additional requirements for Authorising the use of Juveniles as CHIS:

The use of juveniles as CHIS is regulated by the Regulation of Investigatory Powers Act (Juveniles) Order 2000. These regulations provide that when seeking an authorisation the Investigating Officer must:

- (a) make a risk assessment to demonstrate that the physical and physiological risks have been identified and evaluated and explained to CHIS, and
- (b) that an appropriate adult will be present at meetings of any CHIS under 18.

There is a prohibition on a CHIS under the age of 16 being used if a person under surveillance is a parent or has financial responsibility for that CHIS.

#### **4.6 *Obtaining Judicial Approval of Authorisations***

4.6.1 Authorising Officers must when making authorisations be aware that each authorisation (or renewal of an authorisation) will be subject to judicial approval. The Protection of Freedoms Act 2012, amends RIPA, to require that where a Authorising Officer has granted an authorisation for the use of directed surveillance or for the use of covert human intelligence sources, judicial approval will be required.

4.6.2 The Authority will be required to make an application, without giving notice, to the Magistrates' Court. The Magistrates will give approval if at the date of the grant of authorisation or renewal of an existing authorisation if and only if, they are satisfied that:

- (a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these grounds still remain;
- (b) the "relevant conditions" were satisfied in relation to the authorisation. Relevant conditions include that:
  - (i) the relevant person was designated as an Authorising Officer;
  - (ii) it was reasonable and proportionate to believe that using covert surveillance or a covert human intelligence source was necessary and that the relevant conditions have been complied with;
  - (iii) the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25(3) of RIPA; and

- (iv) any other conditions provided for by an order made by the Secretary of State were satisfied.

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

4.6.4 No activity permitted by the authorisation granted by the Authorising Officer may be undertaken until the approval of the Magistrates' Court to that authorisation has been obtained. To ensure compliance with this requirement, any Authorising Officer who proposes to approve an application for the use of directed surveillance or for the use of a covert human intelligence source must immediately inform the Legal Services Manager by telephone or e-mail of the details of the authorisation. The Legal Services Manager will then make the necessary arrangements for an application for an order to approve the authorisation to be made to the Magistrates' Court. The Authorising Officer and the Investigating Officer may be required to attend the Magistrates' Court to support the application.

#### 4.7 ***Cases where Authorisations must be obtained from Specifically Designated Officers***

##### 4.7.1 Confidential Information

Note that where an authorisation for a CHIS is sought and it is likely through the conduct of the CHIS that confidential information would be obtained, then a higher level of authorisation is required. i.e. authorisation by the Chief Executive or by a Director of Services.

"Confidential Information" consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

##### 4.7.2 Legally Privileged Information

This is any communication or information passing between a subject and their legal advisors. It is considered to be particularly sensitive. It is unlikely that such information obtained from CHIS would be admissible in evidence in criminal proceedings. Action which may lead to legally privileged information being obtained by a CHIS is subject to additional safeguards. Investigating officers seeking to obtain such information must refer to the Home Office Covert Human Intelligence Sources Code of Practice.

##### 4.7.3 Confidential Personal Information

This is information held in confidence concerning an individual who can be identified from it (whether living or dead) relating to their physical or mental health or to spiritual counselling or assistance to which a person has had recourse.

#### 4.7.4 Confidential Journalistic Material

This is material acquired or created for the purpose of journalism or communications resulting in information being so acquired and held subject to an undertaking to hold it in confidence.

#### 4.7.5 Use of Juveniles as CHIS

Note that an authorisation as to the use of a juvenile as a CHIS may only be made by the Chief Executive or in his absence the Director of Services.

### 4.8 *Duration, review, cancellation and renewal of authorisations*

- 4.8.1 Regular reviews of authorisations must be undertaken to assess the need for the surveillance to continue. The Authorising Officer must determine how often a review should take place. Reviews should be undertaken by an authorising officer as frequently as s/he considers necessary and practicable. Bearing in mind the intrusive nature of surveillance the presumption must be in favour of early reviews. In any event a review must take place no later than one month after the date of the authorisation/renewal or last review. The reviews should review the continued necessity and proportionality of the authorised covert activity and a record of the review be kept. Periodic reviews are important – they keep the momentum on the investigation and should ensure that intrusions into privacy are kept to a shorter period as possible.
- 4.8.2 The Authorising Officer must cancel an authorisation as soon as he or she believes that the activity is no longer necessary or proportionate. Authorisations do NOT lapse automatically – they must be formally cancelled. Once an investigation has been completed or the circumstances of the case dictate that it must be closed, the Investigating Officer must complete a cancellation of authorisation form and submit it to the Authorising Officer who granted or last renewed the authorisation. Upon cancellation all the original documentation in relation to the authorisation must be forwarded by secure means to the Senior Responsible Officer. The Authorising Officer may cancel the authorisation if he considers that the requirements of the authorisation are no longer satisfied. The Authorising Officer who granted a CHIS authorisation must cancel it if s/he is satisfied that the use of the CHIS no longer meets the criteria for authorisation.
- 4.8.3 A written authorisation for directed surveillance granted by an authorising officer and judicially approved will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time at which it took effect. Urgent oral authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted. If at any time before an authorisation for directed surveillance would cease to have effect the authorising officer considers it is necessary for the authorisation to continue for the purpose of which it was given he may renew

it in writing for a further period of three months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours. Both procedures are subject to the requirement for judicial approval. The Code of Practice recommends that renewal occurs shortly before the authorisation period is drawing to an end. Due to the need for judicial authorisation the renewal process should be undertaken during the last 2 weeks of the current authorisation period. Paragraph 5.12 – 5.16 of the Code relating to covert Surveillance and Property Interference provides more information on renewals.

4.8.4 With regard to an authorisation for the use of CHIS a written authorisation will, unless renewed, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect, except in the case of a juvenile CHIS which lasts for one month. Urgent oral authorisations will, unless renewed, cease to have effect after 72 hours beginning with the time when the authorisation was granted. A renewal can be granted for a further same period and the same procedure as outlined in 4.9.3 applies. When considering an application for renewal of an authorisation for a CHIS the Authorising Officer must consider:

- (a) the use made of the source in the period since the grant or latest renewal of the authorisation; and
- (b) the task given to the source during that period and the information obtained from the conduct or use of the source. The Authorising Officer must be certain that all of the information which was presented to justify the original authorisation is still subsisting and relevant. This applies to authorisations both for directors of surveillance and for use of CHIS.

Paragraphs 5.17 to 5.22 of the Code relating to CHIS provides more information on renewals.

4.8.5 To assist with the proper review, renewal and cancellation of an authorisation the Investigating Officer should keep the following record and diarise the dates for renewal and cancellation:

- (a) a copy of the authorisation together with supporting documents;
- (b) a copy of any renewal of any authorisation together with supporting documents;
- (c) any authorisation which was granted or renewed orally (an urgent case) and the reason why the case was considered to be urgent ;
- (d) any risk assessment raised in relation to a CHIS ;
- (e) the circumstances in which tasks were given to the CHIS;

- (f) the value of the CHIS to the investigation;
- (g) a record of the results of any reviews of the authorisation;
- (h) the reasons for not renewing an authorisation;
- (i) the reasons for cancelling an authorisation; and
- (j) the date and time when any instructions were given by the authorising officer since using a CHIS.

The Investigating Officer should diarise the dates for review of each authorisation.

#### **4.9 *Maintaining Records of Authorisations, Renewals and Cancellations***

- 4.9.1 The Authorising Officer must send the originals of all records of authorisations, renewals and cancellations to the Senior Responsible Officer who will keep a central record. The Unique Reference Number (URN) required on the paperwork must bear a prefix indicating which service the paperwork has originated from (e.g.EH for Environmental Health or A for audit).
- 4.9.2 All of the information relating to the authorisation will form part of the records of the investigation and must be kept on the appropriate file for 5 years or longer if appeals are made.
- 4.9.3 Information that may be of value in connection with concurrent investigations may be kept, but information not relevant to those enquiries must be destroyed.
- 4.9.4 The Senior Responsible Officer will provide a Unique Reference Number for each RIPA application, upon request by an Investigating Officer. He will maintain a central record of all RIPA authorisations, renewals and cancellations. In addition, he will review the authorisations/renewals made on a regular basis to ensure that such authorisations/renewals are made properly, are appropriate and that all forms have been fully completed. He will be able to provide advice on RIPA issues to Investigating and Authorising Officers.

## 5. General

### 5.1 *The Senior Responsible Officer*

The Democratic Services Manager who is also the Council's Monitoring Officer is the Council's appointed Senior Responsible Officer for RIPA. He has responsibility for the integrity of the process to authorise directed surveillance, to ensure compliance with the Act and the Codes of Practice, to engage with the Commissioners and Inspectors when they conduct inspections, to oversee the implementation of any post-inspection action plan recommended or approved by a Commissioner and to ensure all Authorising Officers are of an appropriate standard in the light of any concerns raised by an inspection.

### 5.2 *Chief Surveillance Commissioner*

The Chief Surveillance Commissioner reviews the exercise and performance of the use of authorisations by public bodies.

Information must be provided on request and inspections re carried out regularly by the Surveillance Commissioner.

A tribunal has been established to consider and determine complaints relating to the exercise of RIPA powers by any person aggrieved. The tribunal deals with these matters in a similar manner to the courts when dealing with judicial review cases. Complaints must be lodged with the tribunal within one year unless the tribunal determines it is just and equitable to extend that period.

The tribunal may order the quashing or cancellation of any authorisation, records or information obtained by use of an authorisation.

The Council is under a duty to disclose to the tribunal all documents that may be required relating to the authorisation.

### 5.3 *Officer training*

Relevant officers received a day's training from ITS Training (UK) Limited on the 26<sup>th</sup> March 2012 which covered surveillance law and rules and the use of worked examples particularly around the completion of forms requesting authorisation. It is intended to repeat that training in early 2013 to bring officers up to date with the changes in the law. A register of those attending such training should be maintained.

Unique Reference Number	
-------------------------	--

## Part II of the Regulation of Investigatory Powers Act 2000

### Authorisation Directed Surveillance

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

Unique Reference Number	
-------------------------	--

**DETAILS OF APPLICATION**

**1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521.<sup>1</sup>**

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

**3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.**

**4. The identities, where known, of those to be subject of the directed surveillance.**

- Name:
- Address:
- DOB:
- Other information as appropriate:

**5. Explain the information that it is desired to obtain as a result of the directed surveillance.**

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

Unique Reference Number

6. Identify on which grounds the directed surveillance is **necessary** under Section 28(3) of RIPA. Delete those that are *inapplicable*. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).

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

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

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

Describe precautions you will take to minimise collateral intrusion.

Unique Reference Number

--

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

--

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

--

Unique Reference Number	
-------------------------	--

**11. Applicant's Details**

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

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

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

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

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

<b>Unique Reference Number</b>	
--------------------------------	--

--

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

--

--

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

**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.**

--

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

Unique Reference Number	
-------------------------	--

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

**16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.**

<b>Name (Print)</b>		<b>Grade/ Rank</b>		
<b>Signature</b>		<b>Date and Time</b>		
<b>Urgent authorisation Expiry date:</b>		<b>Expiry time:</b>		
<i>Remember the 72 hour rule for urgent authorities - check Code of Practice.</i>	e.g. authorisation granted at 5pm on June 1 <sup>st</sup> expires 4.59pm on 4 <sup>th</sup> June			

Unique Reference Number	
-------------------------	--

## Part II of the Regulation of Investigatory Powers Act 2000

### Renewal of a Directed Surveillance Authorisation

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

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

**Details of renewal:**

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

Renewal Number	Date

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

<b>Unique Reference Number</b>	
--------------------------------	--

--

**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.**

--

**7. Applicant's Details**

<b>Name (Print)</b>		<b>Tel No</b>	
---------------------	--	---------------	--

Unique Reference Number	
-------------------------	--

Grade/Rank		Date	
Signature			

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

<b>9. Authorising Officer's Statement.</b>
--

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

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

Name (Print)	-----	Grade / Rank	-----
Signature	-----	Date	-----
Renewal From:	Time:	Date:	

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

Unique Reference Number

## Part II of the Regulation of Investigatory Powers Act 2000

### Review of a Directed Surveillance authorisation

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

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

**Details of review:**

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

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

Unique Reference Number

--

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

--

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

--

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

--

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

--

**7. Applicant's Details**

Name (Print)		Tel No	
Grade/Rank		Date	

Unique Reference Number

Signature

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

9. Authorising Officer's Statement.

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

Name (Print)

Grade / Rank

Signature

Date

10. Date of next review.

**Part II of the  
Regulation of Investigatory Powers Act 2000**

**Cancellation of a Directed Surveillance authorisation**

<b>Unique Reference Number</b>	
--------------------------------	--

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

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

**Details of cancellation:**

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

--

<b>Unique Reference Number</b>	
--------------------------------	--

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

<b>3. Authorising officer's statement.</b>
I, [Insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.
<b>Name (Print)</b> _____ <b>Grade</b> _____
<b>Signature</b> _____ <b>Date</b> _____

<b>4. Time and Date of when the authorising officer instructed the surveillance to cease.</b>
<b>Date:</b> _____ <b>Time:</b> _____

<b>5. Authorisation cancelled.</b>	<b>Date:</b> _____	<b>Time:</b> _____
------------------------------------	--------------------	--------------------

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

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

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

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

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

--

DETAILS OF APPLICATION
<b>1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. <sup>1</sup> Where appropriate throughout amend references to the Order relevant to your authority.</b>
<b>2. Describe the purpose of the specific operation or investigation.</b>
<b>3. Describe in detail <u>the purpose</u> for which the source will be tasked or used.</b>
<b>4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.</b>
<b>5. Identify on which grounds the conduct or the use of the source is <u>necessary</u> under Section 29(3) of RIPA. Delete those that are <i>inapplicable</i>. Ensure that you know which of these grounds you are entitled to rely on (eg. SI 2010 No.521).</b>
<ul style="list-style-type: none"><li>• In the interests of national security;</li><li>• For the purpose of preventing or detecting crime or of preventing disorder;</li><li>• In the interests of the economic well-being of the United Kingdom;</li></ul>

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

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

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

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

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

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

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

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

9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.14).

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

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

References for any other linked authorisations:

12. Applicant's Details.

Name  
(print)

Grade/Rank/Position

Signature

Tel No:

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

Date

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

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

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

**16. Date of first review:**

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

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

--

**18. Authorising Officer's Details**

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

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

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

--

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

--

**21. Authorising Officer of urgent authorisation**

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

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

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

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

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

(Please attach the original authorisation)

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

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

**Details of renewal:**

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

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

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

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

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

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

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

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

<b>use of the source.</b>

<b>7. Detail the results of regular reviews of the use of the source.</b>

<b>8. Give details of the review of the risk assessment on the security and welfare of using the source.</b>

<b>9. Applicant's Details</b>			
<b>Name (Print)</b>		<b>Tel No</b>	
<b>Grade/Rank</b>		<b>Date</b>	
<b>Signature</b>			

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

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

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

--

<b>Name (Print)</b>	<b>Grade / Rank</b>
<b>Signature</b>	<b>Date</b>
<b>Renewal From:</b>	<b>Time:</b>
	<b>Date:</b>
	<b>End date/time of the authorisation</b>

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

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

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

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

### Review of a Covert Human Intelligence Source (CHIS) Authorisation

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

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

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

Details of review:

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

Review Number	Date

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

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

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

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

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

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

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

8. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

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

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

Name (Print)	.....	Grade / Rank
Signature	.....	Date

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

**Date of next review:**

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

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

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

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

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

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

**Details of cancellation:**

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

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

**3. Authorising officer's statement. THIS SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.**

Name (Print) \_\_\_\_\_

Grade \_\_\_\_\_

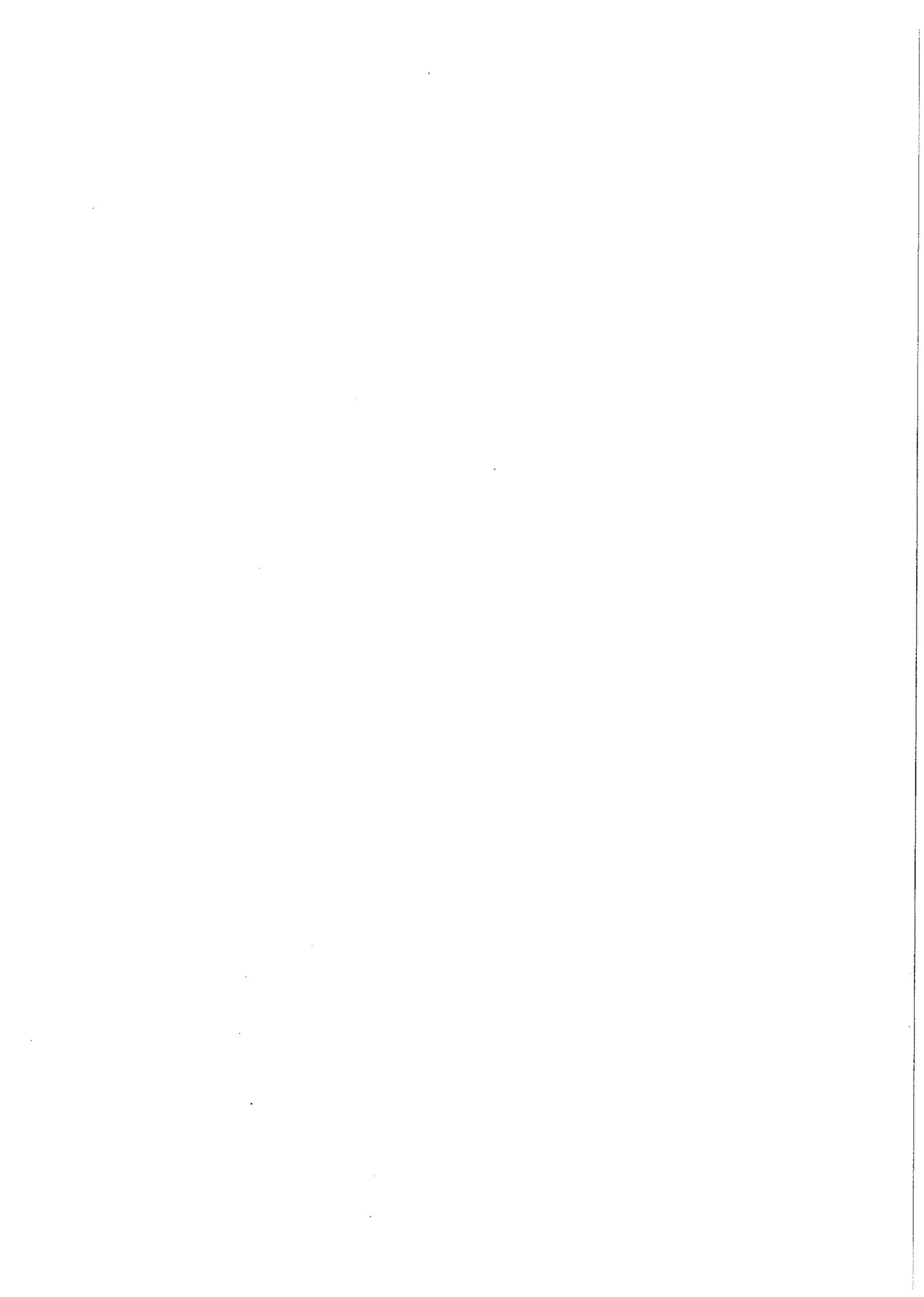
Signature \_\_\_\_\_

Date \_\_\_\_\_

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

Date:

Time:



*Currently being update to reflect legislation changes and to incorporate it into the policy rather than as a separate appendix as recommended by the OSC inspection report*

## Appendix 2

### **GUIDANCE NOTES FOR APPLICANTS (REQUESTING/INVESTIGATING OFFICERS) AND AUTHORISING OFFICERS**

Please use this in conjunction with the current RIPA Policy and Guidance issued by the Council, together with a careful examination of the Codes of Practice.

CONSIDERATION OF THE NOTES IS NO SUBSTITUTE FOR A FULL CONSIDERATION OF THE CODES OF PRACTICE WHICH HAVE BEEN ISSUED TO ALL DEPARTMENTS AND ALL AUTHORISING OFFICERS.

The following notes for guidance relate to completion of applications for directed surveillance.

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

##### Page 1

This should be fairly self-explanatory. Please note that the Senior Responsible Officer will allocate to each authorising officer the directed surveillance unique reference number on each occasion an authorisation is required. This must only be done by the Senior Responsible Officer.

The Council's name and address should be inserted in the box marked "public authority".

The officer requesting the application form should fill in their full name, their Department/Section details, their full work address and any contact details. Please note that a requesting officer has to be an officer of the Council. Where the Council is using other agencies/persons in a surveillance operation the application would have to be done on their behalf by an officer of the Council.

If another person is investigating the authorisation, and they are separate from the requesting officer, their details should also be logged.

##### Page 2

##### Details of Application

##### Box 1. Rank/Position of Authorising Officer

These are defined in Statutory Instrument 2010/512 and are a Director, Head of Service, Service Manager or equivalent. The Democratic Services Manager is the Senior Responsible Officer.

Box 2. Describe the Purpose of the Specific Operation or Investigation

Here, the requesting officer should state the reason behind the investigation. For example "the purpose of the operation is to, through the use of CCTV cameras, obtain corroborative evidence that the tenants and/or visitors and/or residents at number 2 Acacia Avenue, Any Town have engaged in instances which have or are likely to cause harassment alarm distress to the neighbourhood for use in possible anti-social behaviour order proceedings without the need for vulnerable members of the community or witness to give direct evidence in Court".

Box 3. Describe in Detail the Surveillance Operation to be Authorised and Expected Duration, including any Premises, Vehicles or Equipment (eg Camera, Binoculars, Recorder) that may be used.

Here, give particulars of the operation, addressing each aspect raised in the title box 3. References to maps and the type of surveillance equipment to be used and where it is sited may also assist the authorising officer in determining whether or not to grant the authorisation. For example "authorisation is sought to install covert CCTV camera on the roof of the Housing Office opposite block 1-7 Acacia Avenue, as marked "A" on the attached map. The type of surveillance camera to be used/its surveillance capabilities are (here, mention such things as its zoom setting, its sight lines or whether it can be angled or set so that its impact/intrusion can be reduced. Can it be set to run at certain times or will it be 24/7 hour observation?). The expected duration of the operation will be two weeks commencing from when this investigation is authorised. The sight lines for the camera will be outside the pavement at number 1 and number 3 Acacia Avenue. In addition, a mobile CCTV unit placed covertly in a Micra car purchased for its covert surveillance capability will be parked outside number 3 Acacia avenue marked "B" on the attached map for the two week duration. It is envisaged to use the cameras 24 hours a day, 7 days a week. The camera in the covert Micra car will be directed outside number 3 and 5 Acacia Avenue for the same period.

Box 4. The Identities, Where Known of those to be the Subject of the Directed Surveillance.

Here, if you have details of names and addresses, please supply that or other information as appropriate. For example "James and Jenny Anti-social address 2 Acacia Avenue, Any Town, Any Place. Date of birth not known. Other information as appropriate it is alleged that residents and/or visitors of James and Jenny to

number 2 Acacia Avenue also engaged in anti-social activities that affect the local community”.

Box 5. Explain the Information that it is desired to obtain as a result of the Directed Surveillance

Here, state what information you want to obtain as a result of the directed surveillance. For example “allegations of anti-social conduct have been made over a two month period against the occupants of number 2 Acacia Avenue, Any Town, Any Place and their visitors and residents. It is hoped that independent, corroborative evidence of this anti-social behaviour court proceedings case such as eviction, demotion of tenancy or injunction in order to address the problems without the need for vulnerable witnesses who have been threatened in the past to attend at Court”.

Box 6. Identify on which grounds the Directed Surveillance is necessary under Section 28(3) of RIPA

WE CAN ONLY AUTHORISE ON ONE OF THE NECESSITY GROUNDS ‘FOR THE PURPOSE OF PREVENTING AND/OR DETECTING CRIME OR OF PREVENTING DISORDER’.

Box 7. Explain and include reasons why this Directed Surveillance is necessary on the grounds you have identified and include reasons why it is necessary to use the covert surveillance in an investigation (Code paragraph 3.4)

Authorising officers (and requesting officers when they complete this form) should have regard to Code of Practice paragraph 3.3. This states that obtaining an authorisation will only ensure that there is a justifiable interference with an individual’s Article 8 Rights if it is necessary and proportionate for these activities to take place. It requires authorising officers to believe that the authorisation is necessary in the circumstances of the particular case for the statutory ground outlined at Box 6.

Authorising officers should ask themselves why it is necessary to use covert surveillance and whether the evidence to be obtained could be obtained in any other way? Is the directed surveillance operation really necessary to what the requesting officer is seeking to achieve? If there are less intrusive means of obtaining the information, then the authorisation should not be granted. For example, the authorising officer can question whether, in the case of anti-social behaviour allegations, have Council officers or Police Officers witnessed anything which would be sufficient to make a decision on the strength of the allegations and the chances of bringing a successful anti-social behaviour case in Court? Would one CCTV camera work? Is there any need to also have a mobile CCTV unit? Is it necessary to have the cameras on for two weeks, when one week may provide the information? Could

the camera or observations be made during a lesser period of time rather than 24 hours a day? Can the alleged perpetrators be asked to comment on the allegations to obtain their version and to see if any admissions etc are made which would negate the surveillance operation?

The above is a non-exhaustive list of examples of what the authorising officer should consider. One example could be "the directed surveillance is necessary for the purpose of preventing or detecting crime or of preventing disorder because there have been threats of violence on at least four separate occasions over the last two months against members of the local community. This has been by the household of number 2 Acacia Avenue and includes one threat to kill".

It is not deemed safe to at this stage tell the perpetrators about the allegations as this would identify the vulnerable elderly witness that they have threatened directly, who remains terrified about their activities.

No Police Officer or Council officer or any other multi-agency worker, when asked, has witnessed these events and because of the nature and the seriousness of the threats and the vulnerability of the complainants, it is deemed necessary to have limited surveillance in this case.

Box 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 the Precautions you will take to Minimise Collateral Intrusion.

PLEASE LOOK AT, REFER TO AND IF RELEVANT, MAKE US OF THE WORDING OR THE RELEVANT CODES OF PRACTICE.

The idea behind the collateral intrusion is to identify who else, apart from the subject of the surveillance can be affected by the nature of the surveillance. Any application for authorisation should include an assessment of the risk of the collateral intrusion and this should be taken into account by the authorising officer when considering proportionality. The authorising officer needs to know by those carrying out the surveillance if the investigation or operation would unexpectedly interfere with the privacy of individuals not covered by the authorisation. If the original is not sufficient, then you should consider amending the current authorisation or having a new one.

A requesting or authorising officer needs to be aware of any particular sensitivity in the local community (eg a request for a CCTV camera near a Mosque on a Friday). Also, we need to be aware of similar activities being undertaken by other public authorities that could impact on our design to deploy surveillance.

The requesting officer should carry out an assessment of what information could be received. The requesting officer should address their mind as to what may be a consequence of the surveillance and have a plan for if it occurs, for example, "in relation to the covert CCTV camera on the housing office, any potential collateral

intrusion is any visit and/or occupant of number 1, number 2 and number 3 Acacia Avenue. People walking past the footpath outside those properties and also using the road which separates the housing office from the row of terraces marked 1-5 Acacia Avenue can also be the subject of potential collateral intrusion. The intrusion is unavoidable as that is the least angle of intrusion that the camera can be operated under and it cannot be sighted anywhere else without being obvious to the occupants of number 2, the targets of the surveillance. There are no other buildings around. The precautions taken to minimise the collateral intrusion will be to remind any viewing officers viewing the tape of the target of the investigation. Any evidence to be used in Court or of relevance that show people not directly relevant to the investigation will be pixilated out to reduce intrusion into their lives. Officers will be reminded that they can always stop viewing the tape if they capture information which is unavoidably intrusive in their opinion, without seeking further clarification or advice from the authorising officer and/or Legal Services Manager.

Box 9. Explain why this Directed Surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or others? Any why this is intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? (Code paragraph 3.6)

Requesting and authorising officers should have regard for paragraph 3.6 of the Code of Practice.

This involves the authorising officer balancing the intrusiveness of the activity on the target and others who might be affected by it against the need or the activity in operational terms. It will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. Activities should be carefully managed to meet the objective in question and must not be arbitrary or unfair. If it is any of those things, AN AUTHORISATION SHOULD NOT BE GIVEN.

On the example given, the authorising officer could question whether two CCTV cameras were needed (one mobile unit and one on the roof?) which one will be least intrusive? Could we set the angle/times etc to make it proportionate?

The authorising officer should also be provided with information and address their minds to the nature of the complaints or why it is considered proportionate. For example, if there had been one minor allegation of anti-social conduct, it would not be proportionate to authorise covert surveillance by two cameras for two weeks in front of the curtilage of three houses. An example of how to fill in the box may be

“there has been a continuous period of anti-social behaviour complaints against the household of number 2 Acacia Avenue for over a three month period. Previous attempts to obtain information to corroborate the complaints and to provide relief to the complainants have so far failed. Other agencies have been asked if they have witnessed anything which would negate the need for covert surveillance in this way. The effect on the complainant is severe. There are three complaints in this area – the tenants of number 1 and number 3 Acacia Avenue and the elderly mother of the tenant of number 1 who lives with her. The elderly mother is in her 80’s, has a heart condition as a result of threats to kill, which have allegedly been repeatedly made against her and her medical advisors have warned that if she is subjected to more stress without resolution of this matter, she may have a fatal heart attack. The Police in their opinion believe that the residents of number 2 Acacia Avenue are capable of carrying out violent incidents. They have previous convictions for violence and disorder. The other complainant at number 3 Acacia Avenue has developed sleeping problems and is currently off sick from work from work through nervous exhaustion because of the allegations of anti-social behaviour by the complainant. The tenant wants to move. In addition, there have been 10 anonymous phone calls made to the Council’s Anti-Social Behaviour Reporting Hotline, begging for assistance and making similar threats that the residents of number 2 Acacia Avenue have threatened to cause violence to people in the area, and will petrol bomb the house of any complainant who they found grassing on them to the Police or providing any information to them.

The planned surveillance is of a limited duration for a two week period and it is deemed it will not unexpectedly interfere with the privacy of individuals not covered by authorisation. No other similar activities are currently being undertaken by other public authorities in the area at present, eg the Police to the best of the Council’s knowledge. When balancing the needs of the complainants and members of the community, the directed surveillance sought is deemed to be proportionate.

Box 10. Confidential Information (paragraph 4.1 to 4.31) Indicate the likelihood of acquiring any confidential information.

Please read the relevant Codes of Practice paragraphs quoted. It is unlikely in view of the nature of the surveillance that the Council undertakes that this box will be completed. IF IT IS LIKELY, THEN PLEASE PUT “NONE” OR “NONE LIKELY”. DO NOT LEAVE THIS BOX BLANK. If you are in any doubt, then please seek the advice of the Senior Responsible Officer at the earliest opportunity and before any surveillance activity is authorised or carried out.

Box 11. Applicant's Details

Repeat the details given of the applicant or requesting officer. Please put the date and signature as requested.

Box 12. Authorising Officer's Statement (Spell out the 5W's (who, what, where, when, why) and how in this and the following box)

I hereby authorise directed surveillance to find 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 to be achieved?).

Here, follow exactly three prompts in the box. Please do not miss any out and please be as full as possible so that anyone examining the authorisation and more importantly, the requesting officers and people carrying out the investigation will know exactly what their parameters are and why you have authorised this in the manner that you have.

For example "I hereby authorise directed surveillance to find as follows:

I authorise the use of a mobile CCTV camera to be situated at "B" on the attached plan. I authorise it to be set so that its angle can see outside the pavement of number 1, 2 and 3 Acacia Avenue only as marked between the sight level angles I have pencilled in on the attached plan. The surveillance is necessary because very serious allegations and threats have been made by three separate complainants. Also, other complainants have anonymously complained with similar corroborative evidence. The level and nature of the threats and the appropriate response in terms of Court procedure without having to subject vulnerable intimidated witnesses to Court proceedings which will result in their being identified make this surveillance operation necessary. It cannot be achieved by other means. For example, the complainants cannot be discussed at this stage with the alleged perpetrators without putting the complainants in danger. The alleged perpetrators have previous convictions for violence and have made threats of violence against anybody who complains against them and the Police believe that they are capable of carrying

those out. The surveillance will take place for a period of 24 hours a day by use of the CCTV camera only as stipulated above. It is necessary to have it recording for that period of time and because the nature of the logs show that threats and anti-social conduct happen at any time during the day and night. The surveillance is directed against Jenny and James Anti-Social, the joint tenants of number 2 Acacia Avenue. However, there have also been complaints against their associated who visit the household. The surveillance is also aimed at them”.

The particular camera to be used in the Micro is (provide technical details).

Box 13. Explain why you believe the Directed Surveillance is necessary (Code paragraph 3.3. Explain why you believe the Directed Surveillance to be proportionate to what is sought to be achieved by carrying it out (Code paragraphs 3.4 to 3.7)

In relation to necessity, this has been addressed at Box 12.

“In relation to proportionality, I have balanced the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The intrusiveness of the target is the capability of viewing the activities of the occupants and/or visitors to number 2 Acacia Avenue. Also, others not directly targeted by the investigation can include any visitor and/or occupant of number 1 and number 3 Acacia Avenue, and anyone using the footpath that runs outside the house.

I am not aware of any other surveillance activities that are currently being undertaken in the area which may increase the level of collateral intrusion.”

The activity will be carefully managed in that the tapes will be viewed on a daily basis. The officers will be reminded of the focus of the investigation. If they view anything which does not concern the focus of the investigation which they regard of a very private nature impinging on somebody else, they should stop viewing immediately and seek further advice from me as the authorising officer before continuing the viewing.

Given the effect on the complainants' lives (one lady is elderly and is in danger of having a fatal heart attack/another person is off sick with stress and wishing to move) I deem it proportionate to authorise the surveillance I have but only for a period of one week before review.

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

See information provided in relation to confidential information about Box 10. The relevant authorising officer should seek the advice from the RIPA Co-ordinators and/or the Legal Services Officers before completing the confidential information authorisation box.

#### Date of First Review

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

Paragraph 3.22 of the Code of Practice makes it clear that regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central register of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

Paragraph 3.23 makes it clear that it is the task of the authorising officer to determine how often a review should take place. It should be as frequently as is considered necessary and practicable.

Therefore, set the date of the first review for when you think that the requesting officer should have obtained sufficient information to have achieved the aim of their investigation without unnecessary intrusion or imbalanced intrusion into others lives. Bear on the side of caution. Setting a review date earlier is better than setting a review date later when you are not sure for how long it will be necessary and proportionate.

Authorising officer, name, signature and date and time of authorisation.

Here, the authorising officer should put their name, sign the form and put their grade and rank. The date and time of the authorisation should be noted.

**PLEASE TAKE SPECIAL CARE TO AUTHORISE FOR THE SET PERIOD OF THREE MONTHS FOR DIRECTED SURVEILLANCE AUTHORISATION.**

**DO NOT AUTHORISE INADVERTENTLY FOR THREE MONTHS AND ONE DAY.**

Please note that all authorisations last for three months. They should be cancelled as soon as they are no longer necessary and proportionate. Authorisations do not expire. Even if they are deemed necessary and proportionate throughout the whole three month period, they should still be cancelled using the appropriate form.

Urgent Authorisation (Code paragraphs 5.5 and 5.6) Authorising Officer:

Explain why you considered the case so urgent that an oral instead of a written authorisation was given.

There is provision in section 22(6)(c) of the Regulation of Investigatory Powers Act 2000 (immediate response provisions) for an oral urgent authorisation to be given which would cease to have an effect after 72 hours. Although the majority of authorisations will be non-urgent, here, the authorising officer should explain why the case was so urgent that an oral instead of a written authorisation was given.

For example, there had been another threat to kill the next door neighbour and tensions in the area were rising so rapidly, it was deemed that urgent action was required.

Box 16. If you are only entitled to act in urgent cases explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

Please note that for local authorities, only those of the level of authorising officers can act in urgent cases. There are no "deputies" appointed for urgent authorisations as there is for some other agencies using RIPA.

#### Record keeping after the authorisation is granted.

All original authorisations should be submitted as soon as possible to the Senior Responsible Officer and IN ANY EVENT WITHIN ONE WEEK. A copy is to be retained by the authorising officer.

The Senior Responsible Officer will check authorisations and if these are inadequate he will contact the authorising officer for the matter to be put right immediately.

The authorising officer in conjunction with the Head of Service should ensure that the officers carrying out the surveillance (whether they be Council employees or third parties employed/engaged by the Council to carry out the work) understand and are aware of the nature of the surveillance and its limitations.

Applications should be reviewed regularly, can be renewed and should be cancelled as soon as the need has gone, using the appropriate forms which will also have accompanying notes for guidance.

#### **CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION**

Please have regard to paragraph 5.17 of the Code of Practice.

The authorising officer who granted or last renewed the authorisation **must cancel it** if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the authorising officer is no longer available this duty will fall on the person who has taken over the role of the authorising officer or who was acting as authorising officer.

Also see Code of Practice 5.18. As soon as the decision is taken that directed surveillance should be discontinued the instruction must be given to those involved to stop all surveillance of the subjects. The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation where relevant.

Please note that directed surveillance authorisations do not expire. They should be cancelled as soon as the need has gone and it is no longer proportionate to carry out the activity balanced against the intrusiveness on the target and others not directly affected by it.

If a directed surveillance authorisation is needed for the full 3 month period, it should still be cancelled. The forms do not lapse.

Please use the form in the pack. The cancellation should be self-explanatory. When filling out eg the value of surveillance and the operation – please have regard to comments made in the notes for guidance for reviewing authorisations. Similar considerations can be borne in mind.

### Housekeeping

As soon as an authorisation is cancelled, please tell the Senior Responsible Officer so that the central register can be updated. In any event this must be done within 1 week.

All officers engaged in the surveillance activity must be notified as soon as the authorisation has been cancelled so that no unauthorised surveillance is carried out inadvertently.

### **RENEWAL OF A DIRECTED SURVEILLANCE AUTHORISATION**

Here, please have regards to paragraphs 5.12 to 5.16 of the Code of Practice.

If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he can renew it in writing for a period of 3 months unless 5.18 applies. (This does not apply to local authorities as it deals with necessity grounds which we do not have access to anymore).

Renewals can be granted in urgent oral cases and last for a period of 72 hours.

According to 5.13, a renewal takes effect at the time at which or day on which the authorisation would have ceased to have effect but for the renewal. An application of renewal should therefore not be made until shortly before the authorisation period is drawing to an end. Any person who can grant a new authorisation can renew an authorisation (eg any authorising officer). Authorisations can be renewed more than once if they continue to meet the criteria for authorisations.

According to paragraph 5.15 of the Code of Practice, all applications for renewal for directed surveillance should record if this is the first renewal or every occasion on which the authorisation has been renewed before; any significant changes to the information given in paragraph 5.8 (ie information to be provided in applications for authorisations); the reasons why it is necessary to continue with it; the content and value to the investigation or operation of the information so far obtained by the surveillance and the results of regular reviews of the investigation operation.

According to paragraph 5.16, authorisations may be renewed more than once if necessary and the renewal should be kept or recorded as part of the central register of authorisations.

For the renewal form itself, the original authorisation should be attached. The details sought are similar to what was required to fill in for the original authorisation form or reviews.

What should be recorded is any significant changes to the information listed in the original authorisation as it applied at the time of the renewal. For example, "Tenant A's mother has now died".

The form however is largely self-explanatory. For further advice please contact the Senior Responsible Officer.

### Housekeeping

As soon as possible after a renewal, please send the original renewal form to the Senior Responsible Officer; the Authorising Officer should retain a copy. The central register can then be updated with the requisite information required by paragraph 8.1 of the Code of practice (ie if the authorisation is renewed, when it was renewed, who authorised the renewal, the name and rank of the authorising officer).

## **REVIEW OF A DIRECTED SURVEILLANCE AUTHORISATION**

### Public Authority/Applicant's Details

Please see the notes for guidance for Directed Surveillance Authorisation. The only matters to add are the date of authorisation of last renewal and the expiry date of authorisation or last renewal and the review number (eg number 1, number 2 etc).

### Details of Reviews

Please complete the number of the review, and the date any reviews were held previously.

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

The requesting officer should summarise what has happened so far, what private information has been obtained and the value of the information obtained so far.

***For example,*** “the mobile CCTV unit has been in place and operational for a period of one week. There has therefore been produced 7 days worth of 24 hour viewing at the place identified by the map attached to the authorisation”.

The information has been valuable to an extent in that it shows Jenny Anti Social making offensive gestures on the pavement outside number 2 Acacia Avenue. Unfortunately, there was a fault on the system and the sound level of the audio recording device did not record any words. It has now been rectified.

The private information that has been obtained is that on the first day of recording, at approximately 4:00pm outside number 1 Acacia Avenue, Jenny Anti Social was recorded hugging a male visitor to the property who had entered the gate of number 2 Acacia Avenue 20 minutes before.

**Box 3 – Detail the reasons why it is necessary to continue with the directed surveillance**

Here, just put down the reasons why the necessity ground is still made out, having regarding to the code of practice.

***For example,*** Complainants’ logs show that there have been 3 further threats since covert surveillance began. One of the timing of the logs equates with the female of number 2 Acacia Avenue being seen to make gestures outside the property of number 1 Acacia Avenue. complainants remain terrified and unfortunately, because the audio level recording on the CCTV camera had not been set at the correct level, no threats could be recorded which could have been used in Court proceedings.

**Box 4 – Explain how the proposed activity is still proportionate to what it seeks to achieve**

Here, linked to the relevant code of practice, gives details of ongoing reasons or cite the continuation of original reasons to justify this.

***For example***, the complainants continue to remain fragile, scared of reprisals, and the tenant at number 3 Acacia Avenue has just been signed off work for a further 2 months because of stress because of the complaints. The doctors of the tenants's mother at number 1 Acacia Avenue remain concerned about her health and the level of complaints and logs are continuing.

**Box 5 – Details of any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring**

The only detail recorded by the camera was the details of private information given in box 2. The information given in the original authorisation in relation to incidents of collateral intrusion further are still valid.

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

No confidential information has been acquired or accessed and there is no likelihood of it being acquired. (If there is likelihood, contact a Legal Services Officer and/or the RIPA Monitoring Officer/Co-ordinator for guidance).

**Box 7 - Applicant's details**

The applicant/requesting officer should give full comments there.

**Box 8 – Review Officer Comments including whether or not the directed surveillance should continue**

Here, the reviewing officer should state their full reasons to justify continuance of the surveillance operation.

#### **Box 9 – Authorising Officer's Statement**

I (insert name of authorising officer) should set out their full reasons for authorising the continuance of the surveillance operation if that is the case.

For example, "I have considered all of the information given by the Applicant in relation to this review. I have had particular regard for the level of private information and the number of times people who have not been the target of the information have been caught by the CCTV cameras.

I note that although 1 log has "tied up" with one shot on the camera, because of a fault on the recording equipment, no sound was recorded which could have captured threats/words and given the evidence required at this stage for a successful ASBO case and/or other successful Court case without the need for vulnerable witnesses to attend at Court. I believe that the directed surveillance should therefore continue."

If the surveillance is authorised to continue following the review, please set the next review date (eg one week). If you believe it should not continue, or should be cancelled immediately, please note down why. Please also sign, date and print your name and rank as given.

#### **Box 10 – Date of Next review**

The authorising officer should be set the date of the next review and communicate that to the reviewing officer.

#### **Housekeeping**

The original review form should be sent to the Senior Responsible Officer as soon as possible and in any event within 1 week of its completion. A copy of the review form should be retained by the Authorising Officer.

The following notes for guidance relate to covert human intelligence sources.

## **APPLICATION FOR AUTHORITY ON COVERT USE OF HUMAN INTELLIGENCE SOURCE**

### Applicant's Details

Follow instructions on Form for Authorisation to carry out Directed Surveillance.

### Authority Required

Follow instructions on Form for Authorisation to carry out Directed Surveillance

Also Note Where a vulnerable individual or juvenile source is to be used, the authorisation **MUST** be given by the Managing Directors or in their absence their nominated deputy (cross-reference Section 5).

### Details of Application

1. Why the instructions of the CHIS is necessary  
Follow the instructions from Form for Authorisation to carry out Directed Surveillance.
  
2. Identity of those involved in the CHIS operation  
Follow the instructions from Form for Authorisation to carry out Directed Surveillance
  
3. Task to be authorised

Follow the instructions in Form for Authorisation to carry out Directed Surveillance.

4. Give an account of the investigation or operation  
Follow the instructions in Form for Authorisation to carry out Directed Surveillance
5. Explain information desired to be obtained as result of the authorisation  
Follow instructions in Form for Authorisation to carry out Directed Surveillance.
6. Explain why the use of a CHIS is proportionate to what it seeks to achieve  
Follow instructions in Form for Authorisation to carry out Directed Surveillance
7. The identity of the CHIS  
In accordance with best practice the true name of the CHIS should be replaced pseudonym. The true identity of the source should be kept separately and securely and accessed only in the most compelling circumstances.
8. Day to day responsibility for the source and his/her security  
The "Handler" must be an officer of the Council (usually of a position below that of the authorising officer) and that person will have day to day responsibility for dealing with the CHIS, recording the information supplied by the CHIS and for monitoring the CHIS's security and welfare. Name the appropriate officer.
9. Who will supervise the use of the source  
The "Controller" must be an officer of the Council and that person will have a general oversight of the use made of the CHIS .

Name the appropriate officer (cross-reference Section 5).

Appropriate Recording Officer

The "Recording Officer" must be an officer of the Council who is given the responsibility for maintaining a record of the use made of the CHIS. Name

the appropriate officer who will create/update the necessary records for the source.

#### 10. Risk Assessment

This is a necessary step before any CHIS task is authorised.

Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the

source, after the cancellation of the authorisation, should be considered at the outset.

THE PERSON DEFINED AT SECTION 29(5)(A) OF RIPA is responsible for bringing to the attention of the person defined at section 29(5)(b) of RIPA any concerns about the person circumstances of the source, insofar as they might affect:

- The validity of the risk assessment
- The conduct of the source, and
- The safety and welfare of the source

Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken whether or not to allow the authorisation to continue.

#### 11. Previous circumstances of the source affecting operation or risk assessment

Name any known.

12. Is a vulnerable individual to be used as a source?  
Cross-reference Section 5 on what is a vulnerable individual. Only the Managing Directors, or (in their absence) their nominated Deputy can authorise the use of a juvenile or vulnerable CHIS
13. Is a juvenile source to be used?  
Cross-reference Section 5 for a definition. NB. A juvenile source CHIS can only be authorised for ONE month. Only the Director or in their absence the Senior Responsible Officer can authorise the use of a juvenile or vulnerable CHIS
14. Appropriate adult responsibility  
For minors, it is good practice to ensure an appropriate adult is involved in meetings. This can be a parent, guardian, older adult, sibling etc.
15. Risk Assessment  
Special regard should be had to any risk of physical or psychological injuries where juvenile sources are involved. See 11 above.
16. Explaining Identified Risks to the source  
Record how and what was said.
17. Tasking where relative guardian or other responsible adult involved  
The Home Officer Code of Practice on CHIS is implicit that no use of CHIS under 16 should be used to get information about their parents or anyone who has parental responsibility over them.
18. Collateral Intrusion  
See Form for Authorisation to carry out Directed Surveillance.
19. Confidential/Religious Material  
Please see Form for Authorisation to carry out Directed Surveillance.

20. Insurance and Health and Safety Considerations

Please see Form for Authorisation to carry out Directed Surveillance.

21. Applicant's Signature and Date

Self-explanatory.

22. Written Record of Urgent Request for Authorisation

See Form for Authorisation to carry out Directed Surveillance.

23. Request Approved/Refused by the Authorising Officer

See Form for Authorisation to carry out Directed Surveillance.

24. Dates of Cessation and Review

See Form for Authorisation to carry out Directed Surveillance.

**NOTES FOR GUIDANCE FOR APPLICATION FOR A RENEWAL OF A COVERT  
USE OF HUMAN INTELLIGENCE SOURCE**

Please see instruction for Renewal of a Directed Surveillance Authorisation. The only changes here are self-explanatory boxes dealing with evaluating any changes to the security and welfare of the CHIS as part of managing the CHIS properly.

**NOTES FOR GUIDANCE FOR CANCELLATION OF AN AUTHORISATION FOR A  
COVERT USE OF HUMAN INTELLIGENCE SOURCE**

Please follow the instructions for Cancellation of a Directed Surveillance Authorisation.

NOTE the additional risk assessment box and the declaration that the authorising officer must sign in relation to CHIS.

This is part of the remaining duty to have regard to the security and welfare of the CHIS even after the authorisation has been cancelled.

## **REVIEW OF A CHIS AUTHORISATION**

Please follow the instructions for Review of a Directed Surveillance Authorisation.

There is an additional box to invite comments on the security and welfare of the source as part of the ongoing monitoring and regard for that.

## **FLOW CHARTS AND GUIDANCE**

### **NOTES FOR GUIDANCE FOR AUTHORISATION TESTS – DIRECTED SURVEILLANCE**

Authorisation will be required for a proposed activity if the answer is “Yes” to all of the following questions.

If the answer is “No” to any of the following questions, the proposed activity falls outside the scope of RIPA.

- 1) **Is the proposed activity “surveillance”?** The Officer must decide whether the proposed activity will comprise monitoring, observing or listening to persons their movements, their conversations or their other activities or communications, recording anything monitored, observed or listened to in the course of the proposed activity and whether a surveillance device will be used.

- 2) **Is it “covert”?** The Officer must decide whether the proposed activity will be carried out in a manner calculated to ensure that the target(s) will be unaware that it is or may be taking place.
- 3) **Is it “directed”?** The Officer must decide whether the proposed activity is for the purposes of a specific investigation/operation.
  
- 4) **Is it likely to result in obtaining private information about this person?**  
The Officer must decide whether any information about the target’s/targets’ private or family life is *likely* to be obtained.

The test is different from “Is there the faintest chance that I will obtain private information.”

- 5) **Is it a “foreseen/planned response”?** The Officer must decide whether the proposed activity is something other than an immediate response in circumstances where it is not reasonably practicable to get authorisation. If the proposed activity has been planned in advance and not just the immediate reaction to events happening in the course of the Officer’s work, it is not unforeseen and requires authorisation if all the answers to questions 1 to 4 have also been “Yes”.

### Determination of Whether DCS Authorisation is Required

Is the surveillance to be carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place?

No

The surveillance is unlikely to covert and authorisation is not required

Yes

Will the surveillance require the presence of an individual or use of a surveillance device on a person's residential premises or private vehicle?

Yes

No

Does the surveillance require the establishment of a personal or other relationship with another person in a covert manner to obtain provide access to or disclose information as a consequence of the relationship?

This may fall within the definition of "intrusive surveillance" – seek advice from Legal Services Manager

No

Yes

This may require an authorisation for a CHIS –refer to the further guidance in this document

Is the surveillance planned as part of a specific investigation or operation?

No

Is information about a person's private or family life likely to be obtained? The likelihood of obtaining such information should be considered in its widest sense

Authorisation for Directed Covert Surveillance is unlikely to be required

'es

## Determination of Whether CHIS Authorisation is Required

Is a personal or other relationship likely to be established in order to obtain, provide access

No

Yes

A CHIS Authorisation is unlikely to be required

Is the relationship to be conducted

No

Yes

A CHIS Authorisation is

Is the person who is establishing the

Yes

Special rules apply to  
Juveniles –

No

Is the person who is establishing  
The relationship a Copeland  
Borough Council employee or an

No

Yes

Special rules apply to the  
handling  
and control of a CHIS outside the

Authorisation for CHIS.  
should be obtained

The relevant Senior Responsible Officer will keep the records for 5 years to comply with Home Office Guidance.

## **REMINDERS FOR APPLICANTS (THE REQUESTING OFFICERS) AUTHORISING OFFICERS AND SENIOR RESPONSIBLE OFFICER**

### **The Applicant must**

- Read the Corporate RIPA Guidance to staff and be aware of any other guidance issued by the Council's Head of Corporate Resources
- Determine whether or not directed surveillance and or CHIS is required
- Assess whether authorisation will be in accordance with the law
- Assess whether authorisation is necessary under RIPA and whether it could be done overtly
- Consider whether surveillance will be proportionate
- Obtain the RIPA application form and the URN from the SRO
- If a less intrusive option is available and practicable use that option
- If RIPA authorisation is necessary and proportionate prepare and submit the application form to the Authorising Officer
- Review regularly if authorisation is given
- If the operation is no longer necessary or proportionate, complete a cancellation form available from the SRO and submit it to the Authorising Officer
- Send all authorised and any rejected forms, reviews and cancellations to the SRO within 1 week of the relevant event

### **Authorising Officer**

- Consider in detail whether all options have been duly considered
- Consider whether surveillance is necessary and proportionate
- Authorise only if an overt or less intrusive option is not practicable

- Set an appropriate review date (up to 3 months after authorisation) and conduct the review
- Check if surveillance is still necessary and proportionate.
- Review the authorisation on the day(s) set
- Set an appropriate further review date
- Cancel the authorisation when it is no longer necessary or proportionate to need the same
- Keep a copy of all authorisations issued

## SRO

- Read the Corporate Guidance to staff on RIPA and Home Office Codes of Guidance
- Issue the next available URN and appropriate form to the Applicant
- Record the URN on the Register and other details known
- Upon receipt of completed form complete other information on the Register
- Set up a file for each case in URN order
- Regularly review the register and files to ensure no key dates have passed
- Send the Authorising Officer a reminder to undertake a review one week before the due date
- File all forms received and keep the Register up to date
- Ensure that no unauthorised access can be gained to the RIPA files
- Keep the records for a period of 5 years.

