

**SUFFOLK COASTAL DISTRICT COUNCIL**  
**REGULATION OF INVESTIGATORY POWERS ACT 2000**  
**CORPORATE SURVEILLANCE CODE OF PRACTICE**



## **SUFFOLK COASTAL DISTRICT COUNCIL**

### **STATEMENT ON SURVEILLANCE PROCEDURES**

The purpose of this Statement is to ensure that all directed surveillance and use of covert human intelligence sources (CHIS) undertaken by Officers at Suffolk Coastal District Council will be conducted in accordance with the statutory guidance issued by the Home Office and practical advice from the Office of Surveillance Commissioners. By adopting this approach the Council is endeavouring to ensure that there are no breaches of the Human Rights Act 1998 and subsequent legislation known as the Regulation of Investigatory Powers Act 2000. The implications of wrongfully applying such processes will lead to breakdowns in relationships with its stakeholders, the possibility of increased complaints to the Council and Ombudsman and increased claims for compensation payments.

This Statement has been produced under the umbrella of the Anti-Theft, Anti-Fraud and Anti-Corruption Policy agreed by the Council in July 2000, this policy will be reviewed during 2007/08. It is designed to protect the residents of the District and the Officers that are likely to be involved in investigations into the various functions that the Council is required to administer.

The Council has introduced a corporate Code of Practice, relevant supporting documentation and has approved a list of nominated Authorising Officers. The Council's Chief Executive is the responsible Officer for ensuring the proper administration and adoption of relevant procedures. The Audit Partnership Manager (in his absence, the Audit Manager and Data Protection Officer) acts as the central monitoring control for the application of the guidance and the completion of the relevant documentation and registers. The associated documents will be made available to all investigating and authorising Officers along with procedural notes on how to maintain appropriate records.

The Council will ensure that records appertaining to directed surveillance/CHIS are retained whether or not legal action is instigated. These records will be kept for a minimum of five years.

However as a general rule the Council will attempt to ensure that covert surveillance or the use of CHIS (Covert Human Intelligence Sources) is a last resort. Wherever practicably possible the Council will try to ensure that persons subject to investigation are aware of the type of investigation and processes which are to be conducted, thereby reducing the need for application of this policy.

The Office of Surveillance Commissioners undertook a review of the Council's surveillance procedures in June 2003 and this Code reflects the views and advice of the Inspector undertaking the review. The Chief Surveillance Commissioner wrote to the Chief Executive on the completion of the inspection congratulating the Council in using best practice in this field. It is important that we all work towards maintaining this high standard and the application of this Code will be the basis upon which we can achieve this aim.

Trevor Brown (Audit Partnership Manager)  
July 2008

# **SURVEILLANCE A CODE OF PRACTICE**

<b>Contents</b>	<b>Page</b>
Foreword	4
CCTV	4
General	5
Authorisations and product	6
Collateral Intrusion	6
Handling and Disclosure	7
Directed surveillance	7
Authorisation Procedures	8
Special Rules	9
Duration of Authorisations	9
Renewals	10
Cancellations	10
Use of Covert Human Intelligence Sources	10
The Council's RIPA Co-ordinator and RIPA Monitoring Officer	10
Surveillance Log	11
Access to Communications Data	11
The Commissioner's role	12
Corporate Complaints Procedure	12
Permission/Consent Statement for investigations undertaken within or from non-Council premises	13
List of Approved Authorising Officers	14
Summarised General Guidance Notes:	15
<b>Appendices:</b>	
Appendix 1: CCTV Protocol between SCDC and SCS Ltd	
Form RIP 1: Application for the use of authority for Directed Surveillance	
Form RIP 2: Application for renewal of Directed Surveillance	
Form RIP 3: Application for cancellation of Directed Surveillance	
Form RIP 4: Application for review of the use of Directed Surveillance	
Form RIP 5: Register of Requests for Directed Surveillance	
Form RIP 6: Surveillance Log	
Form RIP 7: Application for the use of Covert Human Intelligence Sources	
Form RIP 8: Application for cancellation of the use of Covert Human Intelligence Sources	
Form RIP 9: Application for renewal of the use of Covert Human Intelligence Sources	

## **1. Foreword**

Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals but as a means of protecting the public from harm and preventing crime.

The covert surveillance regulated by the 2000 Act and covered by this code is in two categories: intrusive surveillance and directed surveillance. Authorisation under the 2000 Act gives lawful authority to carry out the appropriate level of surveillance.

Intrusive surveillance is covert surveillance that is conducted on residential places or in private vehicles and/or may be conducted by use of surveillance devices. This is not a power available to the Council and accordingly this Code of Practice will make no further reference to it.

General observation forms part of the duties of many law enforcement officers and other public bodies. Police officers will be on patrol at football grounds and other venues monitoring the crowd to maintain public safety and prevent disorder. Officers may also target a crime "hot spot" in order to identify and arrest offenders committing crime at that location. Trading standards or HM Customs & Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of the 2000 Act.

## **2. CCTV**

Neither do the provisions of the 2000 Act or of this code of practice cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. However there may be occasions when CCTV may be used in a covert manner e.g. for the application of Anti Social Behaviour Orders or at the behest of the Police. In these circumstances authorisations will be required but it is more than likely that these will have to be under the control of the Police and evidence of such must be obtained prior to commencing directed surveillance. There should also be control over the use and retention of the taped material obtained from such operations. This Council has a CCTV protocol with Suffolk Coastal Services Ltd – see appendix 1.

### **3. General**

- 3.1 This code of practice provides guidance on the use of covert surveillance by public authorities under Part II of the 2000 Act.
- 3.2 The code will be readily available, for reference purposes, at the main offices of Suffolk Coastal District Council. It will also be readily available to all Members and Officers of the Council who are involved in directed surveillance operations or procedures.
- 3.3 The 2000 Act provides that the statutory code of practice is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to any court or tribunal considering any such proceedings, it must be taken into account.
- 3.4 There is nothing in the 1994 Act, the 1997 Act or Part II of the 2000 Act comparable to section 17 of the 2000 Act, the effect of which is to exclude intercept material from being adduced in evidence in court proceedings. The carrying out of the surveillance described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996, where those rules apply to the law enforcement body in question.
- 3.5 Except where specified in this code, there is no geographical limitation on where covert surveillance can be conducted. Authorisations can be given for covert surveillance taking place both inside and outside the United Kingdom, although there may be restrictions on authorisations extending to Scotland (see section 46 of the 2000 Act)
- 3.6 In this code:

“2000 Act” means the Regulation of Investigatory Powers Act 2000

“Confidential material” has the same meaning as it is given in sections 98-100 of the 1997 Act.

“Confidential personal information” is information held in confidence concerning an individual (whether living or dead) who can be identified from it, relating:

- to his/her physical or mental health; or
- to spiritual counselling or other assistance given or to be given, and

Information is held in confidence if:

- it is held subject to an express or implied undertaking to hold it in confidence; or
- it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

“Confidential journalistic material” includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking; includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as

well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking;

“Covert surveillance” means surveillance, which is 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;

For the purposes of authorising directed surveillance under the 2000 Act an “authorising officer” means the person designated for the purposes of section 28 of the 2000 Act to grant authorisations for directed surveillance. (see the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order SI 2000/2417.)

- 3.7 Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.
- 3.8 Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient’s medical records.

#### **4. Authorisations and product**

- 4.1 An 'Application for Authority for Directed Surveillance or use of CHIS' must be made through the completion of Form RIP 1 (included within this Code). Authorisation of the application will provide lawful authority for the Council to carry out covert surveillance. Responsibility for authorising surveillance operations will only relate to “directed surveillance” or the use of CHIS. There is no requirement on the part of the Council to obtain an authorisation for a covert surveillance operation and the decision not to obtain an authorisation would not, of itself, make an action unlawful. However, the Council will always seek an authorisation where the purpose of the covert surveillance, wherever that takes place, is to obtain private information about a person, whether or not that person is the target of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenge under the Human Rights Act 1998.
- 4.2 Any person giving an authorisation should first satisfy him/herself that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve. The authorisation of covert surveillance is only required when this is 'necessary' and 'proportionate'. It follows that covert surveillance can never be 'necessary' if the desired information can reasonably be obtained by overt means. Directed surveillance or use of a CHIS is the last resort. The Act in s.80 reinforces this in that, where other powers of enforcement exist under any statute, it endorses such action in its own right unless a RIPA authorisation is required.
- 4.3 The role of the authorising officer becomes pre-eminent. Not only will the officer be the objective judge of necessity and proportionality but he/she will follow through with reviews (to ensure cancellation when the authorisation is no longer justified) - s.45 - and will be alert to the aspect of proportionality which is implicit in intrusion on the privacy of other innocent people caught up in the investigation by way of collateral intrusion.

#### **4.4 Collateral Intrusion**

- 4.5 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special

sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

- 4.6 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. This will be taken into account by the authorising officer, particularly when considering the proportionality of the surveillance.
- 4.7 Those carrying out the covert surveillance should inform the authorising officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.
- 4.8 Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities, which could impact on the deployment of surveillance.
- 4.9 Careful consideration must be taken by Investigating and Authorising Officers when other agencies and combined operations are undertaken. It must be made clear where the responsibility for authorisation lies.

#### **4.10 Handling and disclosure of product**

- 4.11 Officers are reminded of the guidance relating to the retention and destruction of confidential material. To the extent that such material has not been destroyed, the following guidance may be relevant. There should be a central record held in each authority of all authorisations and at this Council it has been agreed that this will be controlled and monitored by the Internal Audit Service. These records and all surveillance material should be retained for a period of at least five years from the ending of the authorisation and until an approved inspection has been carried out by the OSC. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.
- 4.12 If there is any reason to believe that the product obtained during the course of an investigation might be relevant to that investigation or to another investigation or to pending or future civil or criminal proceedings then it should not be destroyed but retained in accordance with established disclosure requirements. Particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996, which requires that material, should be retained if it forms part of the unused prosecution material gained in the course of an investigation, or which may be relevant to an investigation.
- 4.13 RIPA and the Data Protection Act are consistent with each other and accordingly Authorising officers must ensure compliance with the appropriate data protection requirements and relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be retained securely.
- 4.14 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside of Suffolk Coastal District Council, which authorised the surveillance, of any material obtained by means of covert surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

## **5. Directed Surveillance**

5.1 Directed Surveillance is defined in section 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and undertaken:

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

Private information in relation to a person includes any information relating to his private or family life. It would be safe to interpret this in a fairly broad sense.

5.2 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances, which, by their very nature, could not have been foreseen. For example, a Council Officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of his everyday duties.

5.3 Where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle (a tracking device), the activity is classed as directed surveillance and should be authorised accordingly. This is not classed as "intrusive". The attachment of a tracking device to a vehicle is likely to be regarded as *property interference* which can only be authorised by the police.

5.4 Directed surveillance does not include entry on or interference with property or wireless telegraphy. This is not within the powers of the Council.

### **5.5 'Necessity'**

5.6 An application for directed surveillance may be granted by the authorising officer where he believes that the authorisation is necessary:

- for the purposes of preventing and detecting crime or of preventing disorder;

There is a requirement to establish *necessity* the Authorising Officer must be satisfied that it is *necessary* to use *covert surveillance* in the investigation.

### **5.7 'Proportionality'**

5.8 The Authorising Officer must also believe that the surveillance is proportionate to what it seeks to achieve.

"Proportionate" is a very important part of the process and has to be clearly understood by the Authorising Officer. Questions to consider will be, for instance, does the seriousness of the case attract the need for this level of enquiry and/or is this the only way to gather the information required?

'Proportionality' includes the idea of using the least intrusive methods, taking into account the seriousness of the offence and any public health and safety problems concerned.

## **5.9 Authorisation Procedures**

- 5.10 Suffolk Coastal District Council is entitled to authorise directed surveillance as listed in Schedule 1 to the 2000 Act.
- 5.11 Authorising officers should be those of recognised seniority in the Council.
- 5.12 Authorisations must be given in writing by the authorising officer. However, in urgent cases, they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing as soon as is reasonably practicable. This should be done by the person to whom the authorising officer spoke but should later be endorsed by the authorising officer.
- 5.13 Ideally, authorising officers should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently.

## **5.14 SPECIAL RULES**

- 5.15 Information to be provided in applications (RIP 1) for authorisation includes:

A written application for authorisation for directed surveillance should record:

- the identities, where known, of those to be the subject of directed surveillance;
- an account of the investigation or operation;
- the grounds on which authorisation is sought and its necessity (e.g. for the detection of crime or the protection of public health);
- why the directed surveillance is considered to be proportionate to what it seeks to achieve;
- level of authority required or recommended (where that is different);
- an explanation of the information which it is desired to obtain as a result of the authorisation;
- any potential for collateral intrusion;
- the likelihood of acquiring any confidential/religious material.
- And subsequently record whether authority was given or refused, by whom and the time and date.

In all cases there will be a need to evaluate the risks associated with conducting such an investigation and there may also be a need to record such as part of the authorisation.

- 5.16 Additionally, in urgent cases, a written application should record (as the case may be):

- reasons why the case was considered to be urgent;
- reasons why the person entitled to act in urgent cases considered that it was not reasonably practicable for the authorisation to be considered by a person otherwise entitled to act.

5.17 Where the application is oral, the detail referred to above should be recorded in writing as soon as reasonably practicable. The need for applying oral authorisations should always be carefully reviewed and avoided wherever possible.

#### **5.18 Duration of authorisations**

5.19 A written authorisation can only last for a period of three months beginning with the day on which it took effect. It is important that proper review is undertaken by the Authorising Officer at least on a monthly basis (using Form RIP 2 for this purpose). Authorisations should not be allowed to expire at the end of the three month period without properly documented review. An authorisation must be cancelled as soon as it is no longer required.

5.20 Urgent oral authorisations or written 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.

#### **5.21 Renewals**

5.22 If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, he/she may renew it in writing for a further period (by using Form RIP 2) beginning with the day when the authorisation would have expired but for the renewal. This will normally be for a period of 3 months. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

5.23 All applications requests for the renewal of an authorisation for directed surveillance should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- the information as listed in paragraph 5.14 as it applies at the time of the renewal; together with
- any significant changes to the information in the previous authorisation;
- the reasons why it is necessary to continue with the surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- an estimate of the length of time the surveillance will continue to be necessary.

#### **5.24 Cancellations**

5.25 The person who granted or last renewed the authorisation must cancel it if he/she are satisfied that the directed surveillance no longer meets the criteria for authorisation. Cancellations must be authorised by using Form RIP 3.

### **6. Use of covert human intelligence source (CHIS)**

6.1 Circumstances may prevail where the use of a CHIS is required for consideration with an investigation. A CHIS is a person who will participate in gaining information in a covert method direct from the subject. These could be classed as informants, whistleblowers or undercover operatives.

6.2 All authorisations for such operations must only be approved by the Council's Head of Paid Service.

- 6.3 As with standard directed surveillance the CHIS authorisations must be controlled by the Internal Audit Service.
- 6.4 This Authority follows the Code of Practice, Covert Human Intelligence Sources and The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725).
- 6.5 Management of sources involves tasking which is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.
- 6.6 The person referred to in section 29(5)(a) of the 2000 Act will have day to day responsibility for: dealing with the source on behalf of the authority concerned; directing the day to day activities of the source; recording the information supplied by the source; and monitoring the source's security and welfare.
- The person referred to in section 29(5)(b) of the 2000 Act will be responsible for the general oversight of the use of the source.
- 6.7 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a trading standards officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may require authorisation.
- 6.8 It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.
- 6.9 It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and reauthorized (for minor amendments only) or it should be cancelled and a new authorisation should be obtained before any further such action is carried out.
- 6.10 Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.
- 6.11 Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each source.
- 6.12 The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.
- 6.13 In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and

oversight of that source may be taken up by one authority or can be split between the authorities.

## **7. The Council's RIPA Co-ordinator & RIPA Monitoring Officer**

- 7.1 The Audit Partnership Manager has the duty of ensuring that the application of this Code is applied corporately throughout the authority. A copy of all documentation completed by applicants and authorising officers must be provided to the Audit Partnership Manager at the time of completion. As the Council's RIPA Co-ordinator and RIPA Monitoring Officer, the Audit Partnership Manager will maintain a central register of all Directed Surveillance /CHIS requests (by using RIP 5). The Audit Partnership Manager will provide all necessary instruction, advice, guidance and training to those officers completing an application or authorising an application for directed surveillance/CHIS.

## **8. Surveillance Log**

- 8.1 A Surveillance Log (using Form RIP 6) should be fully completed for all aspects of the work undertaken under directed surveillance/CHIS. It is important that each entry is fully completed with the signature of the officer making the record, entering exact time and date where indicated. A complete and accurate record is essential as this document may well be placed before a Court of Law.

## **9. Access to Communications Data**

- 9.1 This section gives guidance on the requirements of RIPA when obtaining communications data from a Communication Service Provider (CSP) and must be read in conjunction with the Accessing Communications Data Draft Code of Practice (<http://www.homeoffice.gov.uk/docs/pcdcpc.html>).
- 9.2 Communications data includes information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself, contents of e-mails or interactions with websites.
- 9.3 All persons engaged in the obtaining of such information will be properly authorised and act with that authority.
- 9.4 Local Authorities may only obtain communications data for the purpose of preventing or detecting crime or of preventing disorder.
- 9.5 The Designated Officer must consider both necessity and proportionality before communications data is obtained.
- 9.6 Access to communications data may be authorised in two ways:
- through an authorisation order in which case the Council will collect or retrieve the data itself; or
  - by a notice in which case a notice is given to the Communication Service Provider (CSP) to collect or retrieve the data and provide it to the Council.
- 9.7 A Designated Officer decides whether or not an authorisation should be granted or a notice given.
- 9.8 The authorisation only authorises the conduct of obtaining communications data. Both the application form and the authorisation are not served on the CSP but are retained by the department.

- 9.9 The authorisation should be in a standard written format and information recorded must include a unique reference number. (See CoP for further information).
- 9.10 Notices are served on the CSP but will only contain enough information allow them to fulfil their duties under RIPA. The notice should also contain the unique reference number.
- 9.11 Oral authorisations may only be made in exceptional circumstances 'for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health'.
- 9.12 Both the applicant and Designated Officer must record oral authorisations at the time or as soon as possible.
- 9.13 Authorisations and notices are valid for one month and this period begins when the authorisation is granted or notice given.
- 9.14 The Designated Officer must cancel all authorisations and notices as soon as they are no longer necessary or the conduct no longer proportionate to what is sought to be achieved. In the case of notices, the relevant CSP operator should be informed of the cancellation.
- 9.15 Applications, authorisations and notices for communications data must be retained until the Communications Commissioner has audited them.
- 9.16 The Council will have at least one person who is the Single Point of Contact (SPOC) whom all notices and authorisations should be channelled through and who will be the only person that deals with the CSPs. The reason for this is that there must be a specific point of accountability in each authority requesting data, not least for oversight purposes, but also should the legality of the request be contested e.g. on human rights grounds. Therefore there cannot be a regional SPOC, or any SPOC, which covers more than one authority although it is allowed to have more than one SPOC with in a Local Authority.
- 9.17 A SPOC will also provide for an efficient regime and assist in reducing the burden on the CSP by such requests.
- 9.18 The SPOC will amongst other things, is able to advise Designated Officers on whether an authorisation or notice is appropriate, the validity of the application and the practicality of obtaining the data.
- 9.19 Under SPOC Training and Assessment Requirements Local Authority an officer can only become a Home Office accredited SPOC after attending 2-day training and undergoing subsequent assessment. Subject to assessment, the Home Office will then issue the SPOC with a PIN number which will be recognised by all CSPs and enable them to access communications data under RIPA.
- 9.20 This PIN number is unique to each SPOC. It is not for the entire Local Authority to use and pass around to different investigators or different investigation departments

## **10 The Commissioner's Role**

- 10.1 The 2000 Act provides for a Surveillance Commissioner to provide independent examination of the use of the powers contained within Part II by the police (including the Service Police and the Ministry of Defence Police), NCIS, the National Crime Squad, British Transport Police, HM Customs & Excise, the Ministry of Defence and HM Armed Forces in Northern Ireland and other public authorities.

- 10.2 This Code does not cover the exercise of the Commissioner's functions. However, it will be the duty of any person who uses these powers to comply with any request made by the Commissioner to provide any information as he requires for the purpose of enabling him to discharge his functions.

## **11 Corporate Complaints Procedure**

- 11.1 The Council operates a Corporate Complaints Procedure and persons who are not satisfied with the methods employed by the Council when conducting investigations in accordance with this Code are entitled to make representation through this, or any other appropriate, process. Details can be obtained from the Suffolk Coastal District Council offices at Melton Hill, Woodbridge or from the website at [www.suffolkcoastal.gov.uk](http://www.suffolkcoastal.gov.uk).

**INVESTIGATIONS PROCEDURE**  
**PERMISSION/CONSENT STATEMENT**

The Council is required to ensure that Officers, conducting investigations on its behalf, comply with the Regulation of Investigatory Powers Act 2000.

Consequently Officers who wish to conduct investigations within, or from, non Council premises are required to receive permission to do so from the appropriate private individual or organisation.

This document is intended to record the granting of such consent.

1. Investigation Reference
2. Officer Requesting Permission
3. Address of Premises/Location of Site
4. Reason for Visit
5. Date of Investigation Visit
6. Person giving Permission
7. Signature of Consenting Person/s
8. Date of Signature

## SUFFOLK COASTAL DISTRICT COUNCIL

### COVERT/DIRECT SURVEILLANCE

#### APPROVED AUTHORISING OFFICERS

In accordance with the Regulation of Investigatory Powers Act 2000 the Council is required to nominate Officers who will authorise and monitor investigations which require covert or directed surveillance. Operations involving the use of Covert Human Intelligence Sources (CHIS) can only be authorised by the Chief Executive Officer.

All authorisations must be registered with the Internal Audit Service who will maintain a central control. These will be periodically monitored to ensure their appropriateness.

These nominated Officers must ensure that the investigation is conducted in accordance with "proportionality" and that proper records, as prescribed, are maintained. Nominated Officers must not be involved with the routine investigations.

<b>Directed Surveillance</b>	<b>Authorising Officers</b>
Internal Audit & Counter Fraud	Mr T Brown: (Audit Partnership Manager) and Mrs S Martin (Audit Manager and Data Protection Officer)
Housing	Mr M Eaton (Head of Service)
Corporate	Mr T Osmanski (Strategic Director)
Environmental Health	Mr P Gore (Head of Service)
Planning	Mr P Ridley (Head of Service)

<b>Covert Human Intelligence Source</b>	<b>Authorising Officers</b>
	Mr S Baker (Head of Paid Service)

<b>RIPA: Single Point of Contact</b>	<b>Authorising Officers</b>
	Mrs S Martin (Audit Manager and Data Protection Officer) Mr D Kennedy (Counter Fraud Manager)

## SUFFOLK COASTAL DISTRICT COUNCIL

### GENERAL GUIDANCE ON APPLICATIONS FOR DIRECTED SURVEILLANCE/CHIS

1. Directed Surveillance/CHIS should be a last resort and only used where there is no alternative legal method of obtaining the appropriate evidence.
2. Overt methods should be used wherever possible – this could entail notifying subjects in advance that certain monitoring processes will be taking place on, or around, certain times and dates. It could also be achieved by openly making site visits and making representation to the subjects.
3. Employees of the Council who could be subject to such investigation can be deemed as being overtly surveyed as long as there is evidence within that persons conditions of employment that random checks of various natures will be undertaken. These may include data matching, compliance with codes of conduct and the use of electronic communications.
4. Investigating Officers must ensure that risk assessments are undertaken of the operations to be performed to ensure the safety of the persons concerned and the legality of the evidence likely to be acquired.
5. Investigating Officers must ensure that application forms are fully completed and provide adequate details of:-
  - The necessity of the action being taken e.g. what would the implications be if the investigation was not continued.
  - Why the action is “proportionate” e.g. does the seriousness of the case warrant such action and/or is there no other legal method of obtaining the information.
  - How the activity is to be carried out
  - What information is likely to be forthcoming
6. Investigating Officers must also ensure that the potential for collateral intrusion is considered (i.e. obtaining information of subjects other than the person/s targeted). Investigating Officers must then consider methods for reducing the risk of collateral intrusion and the possibility of editing the evidence gathered.
7. Investigating Officers must ensure that they do not conduct covert surveillance in such a manner that it can be construed as intrusive i.e. by trespassing onto private land, private residences or private vehicles.
8. Investigating Officers may use other premises to conduct surveillance provided that written permission has been sought from the owner/occupier. However the Investigating Officer must again ensure that there is no intrusion over other private premises/property e.g. by seeing into those premises. It is advised that further guidance be sought prior to these occasions.
9. Authorising Officers must include comments regarding their view of the necessity, proportionality and risk of the assignment.
10. Completed authorisations must be immediately notified to the Internal Audit Service who will register the original document. Investigating Officers must ensure that copies of the authorisation are retained with their working files wherever possible.
11. Internal Audit will periodically review the register to ensure each “live” authorisation is appropriate. This procedure is intended to ensure that investigations are brought to a close and cancelled as soon as is practicable and that “ongoing” authorisations are avoided.

12. Internal Audit will provide a unique reference number to each authorisation which will supplement the Investigating Officers own reference. This should ensure that the Internal Audit Service can maintain a thorough check on all existing authorisations.
13. All authorisations will be retained on both the working and audit files for a minimum of 5 years from the ending of the authorisation and/or until they have been inspected and approved by representatives of the OSC. There may also be a need to retain certain forms for a further period depending on any ongoing legal proceedings.
14. Advice on specific areas of concern should be directed to the Internal Audit Service or the Solicitor of the Council.
15. The aforementioned guidance remains the same for CHIS except in the following instances.
  - A CHIS could be an informant, whistleblower, undercover operative or Officer using highly sensitive sound recorders (DAT machines). These types of situation are likely to be rare but it is advisable that further guidance is obtained prior to recommending action.
  - The Audit Partnership Manager or his designated Deputy the Audit Manager and Data Protection Officer only must approve all CHIS authorisations.
16. Any further advice or guidance required can be obtained from Trevor Brown, Audit Partnership Manager.

# **CCTV Protocol**

**This protocol is to cover the situations under which Suffolk Coastal Services Ltd. (SCS) will deploy the covert CCTV camera within the Suffolk Coastal District Council (SCDC) area on behalf of the said Council.**

The prime function of the CCTV system (hereafter referred to as "the unit") is to detect envirocrime\*<sup>1</sup> and in particular fly tipping. Under certain conditions however, it may be deployed for other legitimate uses. The unit may also be made available to other District, Parish or County Councils or the Police to be used in similar circumstances where criminal activity needs to be detected.

The unit is designed to record criminal activity and for that reason it will often be used covertly. It consists of up to 4 cameras, each capable of recording simultaneous images on DVD. These images are only intended to be used as evidence in Court Proceedings and in some strictly controlled circumstances (see note 11d) for publicity, training or educational purposes. The unit is designed to operate at remote sites over periods of several days. In order to protect the unit from theft or vandalism and the integrity of the system, it will be hidden and camouflaged and no warning notices that CCTV operates in the area will be deployed. Operating in this way means that an application for authorisation of directed surveillance under the provisions of Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) will have to be made in every case.

The unit will be under the general control of the Waste Services Officer / Senior Environmental Health Officer (WSO) who is an officer of both SCDC and SCS. The WSO will refer to the Head of Health (HH), the Operations Manager (OM) or Partnership Manager (PM) for specified conditions detailed below.

In general use the system will be deployed in the following circumstances and conditions:-

1. A "RIPA" application for authorisation of directed surveillance will be made by the WSO. The application will be made to HH, or, in that officer's absence or unavailability, any other authorising officer designated for RIPA purposes at SCDC. The application will be for the unit to be placed at one site for up to a maximum of 21 days at any one time. The unit will not be deployed without the RIPA application being authorised in writing.
2. **Intrusive surveillance will not be carried out.**

3. Each deployment of the unit will be recorded on M3 (Northgate) complaints system by the WSO. All subsequent information relating to the deployment of the unit will be entered on the M3 Northgate system by WSO.
4. The decision to seek permission to deploy the unit in a public place, or on private land with the land occupier's written consent, will be made by the WSO.
5. The prime target for siting the unit will be fly tipping hotspots. For the purposes of this protocol, a fly tipping hotspot is defined as being a single site which has been the subject of flytipping incidents on more than one occasion within the previous year.
6. It is envisaged that whilst the unit will be available for use to detect littering, dog fouling, graffiti, vandalism, fly posting and other similar anti social behavioural activities, it will not generally be used for those purposes. Any deployment for use against these crimes will require the sanction of the WSO and either OM or PM.
7. The unit will usually be sited on land owned or controlled by a District, Parish or County Council. It may be sited on land owned by a Government body (such as The Forestry Commission) or on privately owned land (such as a Supermarket recycling area).
8. The unit will only be deployed in a moving vehicle with the express permission of PM or HH in accordance with RIPA conditions.
9. The unit will be sited in such a way that the prime target area of the cameras will be limited to:-
  - a. Land in Public ownership or under public control. This means land owned by a District, Parish or County Council or by a Central Government body.
  - b. Where the camera is on privately owned land, the prime target area will be within the extent of land controlled by the person making the request and any publicly owned land adjacent.
  - c. Where there is some minor overspill of the recorded images from the target area onto privately owned land, every effort will be made to reduce this to the absolute minimum needed to secure workable pictures of the target area.
  - d. Any images recorded of private property will be "redacted" (altered to prevent recognition) before any image is used, but not where the "master copy" is to be used for legal proceedings as that cannot be altered or edited in any way.

10. Where it is known beforehand that recorded images will include images of the exterior of privately occupied premises, the decision to seek to deploy the unit in those circumstances will only be taken by the WSO in consultation with the OM or PM. Where an application is to be made under these circumstances, the permission of the occupier of the premises must be obtained before the application is submitted.
  
11. Stored images of each incident will be kept for the following periods
  - a. Where there has not been any fly tipping or other criminal activity detected, the images will not be examined or saved and will be deleted.
  - b. Where there has been an incident that warrants further investigation, the images will be examined by the WSO with at least one other person in attendance, to determine if there is sufficient evidence to proceed with any form of legal proceedings. If there is not sufficient evidence to so proceed, the images will not be saved and will be deleted.
  - c. Where there is sufficient evidence to proceed, the WSO will ensure that at least 3 authenticated copies of the recorded images are made. All copies will be securely stored. One (referred to above as "the Master Copy") is provided in an evidence bag for court use only. One will be stored in an evidence bag for controlled use and the third will become the working copy upon which further decisions will be based. Details of these and any other copies made will be recorded on M3 (Northgate) complaint system and if at any time it is decided to not proceed further with the case, the WSO will certify that the copies have all been destroyed before completing and finalising the complaint.
  - d. Where legal proceedings are begun, the copies of images will be kept until the case is determined, whereupon:-
    - i. If the case returns a not guilty verdict, all images will be immediately deleted and the WSO will certify that the copies have all been destroyed before completing and finalising the complaint.
    - ii. If the case returns a guilty verdict, the images will be kept for at least the period in which an appeal may be lodged and if such an appeal is lodged, the images will be kept until the final outcome is attained.
    - iii. If no appeal is lodged, or the guilty verdict is upheld on appeal, the images will be kept for a period of up to 2 years for publicity purposes and for up to 5 years for training or educational purposes only. At the end of these periods, the images will be deleted and destroyed.
  
12. If the unit is used by any other Council, or Government Body outside the Suffolk Coastal District Council area, the above protocol shall apply. In such situations, the

references to "HH" or "SCDC RIPA Authorising Officer" will be construed as being a similar officer in the requesting organisation.

13. This protocol will be reviewed by WSO and OM or PM with a representative of HH:-
  - a. After the first deployment of the unit.
  - b. 6 months after the first deployment.
  - c. Every year thereafter
  - d. At any other time if there is any reason or sustainable request to do so.

Signed on behalf of Suffolk Coastal District Council ..... DATE .....

Signed on behalf of Suffolk Coastal Services Ltd. .... DATE .....

\*<sup>1</sup> **What is Envirocrime?**

**Envirocrime is a term normally given to cover incidents that impact upon the environment in a negative manner including fly-tipping, graffiti, fly-posting, abandoned vehicles and dog fouling. It also includes waste collection and disposal problems such as trade waste storage and escape, or problems with domestic refuse collection such as incorrect or early presentation of waste. Envirocrime can often lead to a spiralling decline in an area giving the impression that neither the Council nor the community care. This in turn can lead to more serious crime as criminals feel that they are in an area where it is safe to operate.**

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>			

#### **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 2003; No. 3171.<sup>1</sup>**

--

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

<b>2. Describe the purpose of the specific operation or investigation.</b>
<b>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.</b>
<b>4. The identities, where known, of those to be subject of the directed surveillance.</b>
<ul style="list-style-type: none"><li>• Name:</li><li>• Address:</li><li>• DOB:</li><li>• Other information as appropriate:</li></ul>
<b>5. Explain the information that it is desired to obtain as a result of the directed surveillance.</b>

**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 2003 No.3171)**

- 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 2.4]**

**8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]**

**Describe precautions you will take to minimise collateral intrusion**

**9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 2.5]**

**10. Confidential information. [Code paragraphs 3.1 to 3.12]**  
 INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

--

**11. Applicant's Details.**

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

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

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

**13. Explain why you believe the directed surveillance is necessary. [Code paragraph 2.4]**

**Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]**

**14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 3.1 to 3.12**

**Date of first review**

**Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.**

**Name (Print)**

**Grade / Rank**

**Signature**

**Date and time**

**Expiry date and time [ e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59 ]**

**15. Urgent Authorisation [Code paragraphs 4.17 and 4.18]: 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	<u>Date</u>

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

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

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

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

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



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

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

### **Cancellation of a Directed Surveillance authorisation**

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

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

**Details of cancellation:**

<b>1. Explain the reason(s) for the cancellation of the authorisation:</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.				
<table> <tr> <td><b>Name (Print)</b> .....</td> <td><b>Grade</b> .....</td> </tr> <tr> <td><b>Signature</b> .....</td> <td><b>Date</b> .....</td> </tr> </table>	<b>Name (Print)</b> .....	<b>Grade</b> .....	<b>Signature</b> .....	<b>Date</b> .....
<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>
------------------------------------	--------------	--------------

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

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

### Review of a Directed Surveillance authorisation

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

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

**Details of review:**

10. Review number and dates of any previous reviews.	
Review Number	<u>Date</u>

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

--

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

--

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

--

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

--

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

--

**16. Applicant's Details**

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

<b>Grade/Rank</b>		<b>Date</b>	
<b>Signature</b>			

<b>17. Review Officer's Comments, including whether or not the directed surveillance should continue.</b>

<b>18. Authorising Officer's Statement.</b>								
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].								
<table style="width: 100%; border: none;"> <tr> <td style="width: 25%;"><b>Name (Print)</b></td> <td style="width: 40%; border-bottom: 1px dotted black;"></td> <td style="width: 15%;"><b>Grade / Rank</b></td> <td style="width: 20%; border-bottom: 1px dashed black;"></td> </tr> <tr> <td><b>Signature</b></td> <td style="border-bottom: 1px dashed black;"></td> <td><b>Date</b></td> <td style="border-bottom: 1px dashed black;"></td> </tr> </table>	<b>Name (Print)</b>		<b>Grade / Rank</b>		<b>Signature</b>		<b>Date</b>	
<b>Name (Print)</b>		<b>Grade / Rank</b>						
<b>Signature</b>		<b>Date</b>						

<b>19. Date of next review.</b>	
---------------------------------	--



Suffolk Coastal District Council

## Surveillance Log

Operation No. / Name	
Surveillance Subject Name	
Officers Involved	Officer 1:
	Officer 2:
	Officer 3:
	Officer 4:
Start Date	
Start Time	
Date Concluded	
Exhibit No. / Reference	
RIPA Authorisation Date	
RIPA Authorisation Reference	
RIPA Cancellation Date	

**A reminder of relevant issues:**

**Amount of Time the Observations took place over**

**Distance of the Observations**

**Visibility Conditions in which the Observations were Made  
Obstacles or Impediments to Vision / Observations**

**Knowledge – Previous Knowledge of the Subject Observed**

**Any Other Reason to Recall the Person or Actions Observed**

**Time Delay between the Observations and the Record**

**Errors in Description**

Time	Date	Place	Observations			

Officer's Signature:		Time of Signature:		Date of Signature:	
-------------------------	--	--------------------	--	--------------------	--



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 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>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>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>			

<b>DETAILS OF APPLICATION</b>
<b>17. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171.<sup>2</sup> Where appropriate throughout amend references to the Order relevant to your authority.</b>
<b>18. Describe the purpose of the specific operation or investigation.</b>
<b>19. Describe in detail <u>the purpose</u> for which the source will be tasked or used.</b>
<b>20. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.</b>
<b>21. 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 inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (eg. SI 2003 No.3171)</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> <li>• In the interests of public safety;</li> <li>• for the purpose of protecting public health;</li> <li>• for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.</li> </ul>

<sup>2</sup> For local authorities: The formal position of the authorising officer should be given. For example, Head of Trading Standards.

**22. Explain why this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 2.4]**

**23. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]**

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

**24. 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 2.9)**

**25. Provide an assessment of the risk to the source in carrying out the proposed conduct. (see Code 2.9)**

**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 paragraph 2.5]**

**11. Confidential information. [Code paragraphs 3.1 to 3.12]  
Indicate the likelihood of acquiring any confidential information.**

References for any other linked authorisations:

**12. Applicant's Details.**

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

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

**14. Explain why you believe the conduct or use of the source is necessary. [Code paragraph 2.4]**

**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 paragraph 2.5]**

**15. (Confidential Information Authorisation.) Supply details demonstrating compliance with Code paragraphs 3.1 to 3.12**

**16. Date of first review:**

**17. Programme for subsequent reviews of this authorisation: [Code paragraphs 4.19 and 4.20]. 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>		Time and date granted* Time and date authorisation ends	

**\* 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 4.17 and 4.18]: 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 4.18]. 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**

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

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

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

**Details of cancellation:**

<b>6. Explain the reason(s) for the cancellation of the authorisation:</b>

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

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

<b>Name (Print)</b>	_____	<b>Grade</b>	_____
<b>Signature</b>	_____	<b>Date</b>	_____

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

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

<b>Unique Number*</b>	<b>Operation</b>	<b>Reference</b>	
(*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>20. Renewal numbers and dates of any previous renewals.</b>	
<b>Renewal Number</b>	<b><u>Date</u></b>

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

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

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

**24. 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.**

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

--

**26. Detail the results of regular reviews of the use of the source.**

--

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

--

**28. Applicant's Details**

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

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

--

**30. 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**

**Renewal From: Time:** ..... **Date:**  
**End date/time of the authorisation**

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

<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>	

**Details of review:**

<b>31. Review number and dates of any previous reviews.</b>	
<b>Review Number</b>	<b><u>Date</u></b>

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

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

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

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

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

--

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

--

**38. Applicant's Details**

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

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

--

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

--

**Name (Print)** ..... **Grade / Rank**

**Signature** ..... **Date**

**Date of next review:**

--



SPoC Office Contact Details and Address

If there is a specific or critical time issue indicated or the matter is DCG Grade 1 or 2 URGENT then the Accredited SPoC details MUST be completed

**TEL**

**FAX**

**EMAIL**

**POSTAL**

**Name of Accredited SPoC**

**Mob TEL**

**Reminder:** If you have requested a "24/7" response from the CSP make sure you supply sufficient contact details so that you and your SPoC colleagues can be easily contacted

**Date Notice served**

**and if appropriate the time**

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

### Application for Communications Data

**This form is to obtain authorisation to issue a RIPA Section 22 Notice to a CSP to release Communications Data**

**Name of Public Authority making this application: \_\_\_\_\_**

<b>1) Applicant's Name</b>		<b>4) Unique Reference Number</b>	
<b>2) Office, Rank or Position</b>		<b>5) Applicant's Telephone Number.</b>	
<b>3) Applicant's Email Address</b>		<b>6) Applicant's Fax Number</b>	
<b>7) Operation Name (if applicable)</b>		<b>8) STATUTORY PURPOSE</b>	
		Click here for options:-	

### **9) COMMUNICATIONS DATA**

**Describe the communications data, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)**

### **10) NECESSITY**

**State why it is necessary in relation to your investigation or operation to obtain this data for the purpose listed at question 8)**

*What do you expect to achieve from obtaining the communications data? Explain why you have requested the specific date/time period. If applicable, explain the time scale within which the data is required to be delivered to you.*

### **11) PROPORTIONALITY**

**State why obtaining the communications data is proportionate to what you are seeking to achieve**

*Why does the intrusion benefit the investigation or operation you are undertaking? When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy?*

--

**12) COLLATERAL INTRUSION**

Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances

*If you have identified any meaningful degree of collateral intrusion, explain what it is.*

--

**13) TIMESCALE**

Identify and explain the timescale within which the data is required

--	--

**14) APPLICANT**

I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data

Applicant's Signature

Date

--	--	--	--

**15) ASSESSMENT BY ACCREDITED SPoC.**

If the request is NOT reasonably practical for the CSP explain why

Specify which sub-section the data falls within

Click here for options:-

State whether notice or authorisation is appropriate

Click here for options:-

Describe any adverse cost or resource implications to either your public authority or the CSP?

If the request will provide any excessive data to that requested by the applicant, give details.

Are there other factors the DP should be aware of?

Name of Accredited SPoC


**16) AUTHORISATION (Completed by Accredited SPoC when appropriate)**

Specify the reason why the collection of communications data by means of an authorisation is appropriate:

- CSP is not capable of obtaining or disclosing the communications data;
- The investigation or operation may be prejudiced if the CSP is required to obtain or disclose the data;
- There is an agreement in place between the public authority and the CSP relating to the appropriate mechanisms for the disclosure of the data;
- The designated person considers there is a requirement to conduct a telephone subscriber check but a CSP has yet to be conclusively determined as the holder of the communications data.

**Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought. Also, describe the course of conduct required to obtain it.**

**Name of the relevant CSP**

**The statutory purpose for which the conduct may be authorised is set out at section 8 of this form. The office, rank or position of the designated person should be recorded within section 17 of this form. A record of the date & time the granting of an authorisation is made should be recorded within section 17 of this form**

## 17. DESIGNATED PERSON

***The Designated Person considers the application and if approved records their considerations:***

*If you, based on this application, **believe** acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act consider the following;*

- Why do you **believe** the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgement you should take in consideration any additional information from the SPoC.*
- Where accessing the communication data is likely to result in meaningful degree of collateral intrusion, why you **believe** the request remains justified and proportionate to the objective(s)?*

**My considerations in approving / not approving this application are:**

- I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form.
- I give Notice and require the SPoC to serve it on (insert name of CSP) . The Notice bears the unique reference number

<b>Name</b>		<b>Office, Rank or Position</b>	
<b>Signature</b>		<b>Time and Date</b>	

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

### Reporting of an Error by Communication Service Provider (CSP)

Name of CSP reporting this error \_\_\_\_\_

**An error can only occur after a designated person (within a public authority):**

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

**Where a CSP discloses communications data in error it must report each error to the Commissioner.**

1) Name of staff member from CSP		4) Telephone Number	
2) Position within the CSP		5) Fax Number	
3) Email Address		6) The error can be reported by email	<a href="mailto:Ch2.inspectorate@homeoffice.gsi.gov.uk">Ch2.inspectorate@homeoffice.gsi.gov.uk</a>

#### 7) DETAILS OF THE ERROR

**State whether Notice or Authorisation;** Click here for options:-

**Describe the communications data sought by the public authority as set out on the Notice or Authorisation;**

**Describe the nature of the error;**

**Date and time the error occurred;** Date                      Time

**If the CSP is reporting an error made by the public authority - Name of public authority ("the PA");**                      **and state whether PA has been informed;**  
Click here for options:-;

#### 8) PREVENTION OF SIMILAR ERRORS REOCCURRING

**What steps have been, or will be, taken to ensure that a similar error does not reoccur**

**9) REPORTING OF THE ERROR TO THE COMMISSIONER AND NOTIFYING PERSON OF SENIOR POSITION WITHIN THE CSP**

**Details of the person of Senior Position (if different from person completing form, see question 1 above)**

**Name**  
**Email address**

**Telephone No**

**The date and time the report has been completed by CSP**

**Date**      **Time**