Appendix A

SOUTH DERBYSHIRE DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY AND GUIDANCE

CONTENTS

SOUTH DERBYSHIRE DISTRICT COUNCIL

POLICY ON REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Introduction

South Derbyshire District Council only carries out covert surveillance where such action is justified and endeavours to keep such surveillance to a minimum. It recognises the importance of complying with RIPA when such an investigation is for the purpose of preventing or detecting crime or preventing disorder and has produced this guidance document to assist officers.

Applications for authority

An officer of ~~at least Unit Manager~~Director level or the Monitoring Officer will consider all applications for authorisation in accordance with RIPA ("the Authorising Officer"). Any incomplete or inadequate application forms will be returned to the applicant for amendment. The Authorising Officer shall in particular ensure that: -

- there is a satisfactory reason for carrying out the surveillance
- the covert nature of the investigation is necessary
- proper consideration has been given to collateral intrusion
- the proposed length and extent of the surveillance is proportionate to the information being sought.
- Chief Executive's authorisation is sought where legal/medical/clerical issues are involved
- The authorisations are reviewed and cancelled.
- Records of all authorisations are sent to the Head of Legal & Democratic Services for entry on the Central Register.

DEPARTMENT	AUTHORISING OFFICER / DESIGNATED PERSON
CHIEF EXECUTIVE'S	CHIEF EXECUTIVE
CORPORATE SERVICES	DIRECTOR OF CORPORATE SERVICES
COMMUNITY SERVICES	DIRECTOR OF COMMUNITY SERVICES
LEGAL AND DEMOCRATIC SERVICES	HEAD OF LEGAL & DEMOCRATIC SERVICES MONITORING OFFICER

Training

Each Authorising Officer shall be responsible for ensuring that relevant members of staff are aware of the Act's requirements.

The Head of Legal & Democratic Services shall ensure that refresher training is offered once a year to all directorates of the Council and also give advice and training on request.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

GUIDANCE - PART I

DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE

1. Purpose

The purpose of this guidance is to explain

the scope of RIPA – Part II;
the circumstances where it applies; and
the authorisations procedures to be followed

2. Introduction

2.1 The Regulation of Investigatory Powers Act 2000 ("the Act"), which came into force in 2000, is intended to regulate the use of investigatory powers exercised by various bodies including local authorities, and ensure that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate Authorised Officer before they are carried out.

2.2 The investigatory powers, which are relevant to a local authority, are directed covert surveillance in respect of specific operations or specific investigations and the use of covert human intelligence sources. The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There are also Codes of Practice in relation to the use of these powers and these are attached at **Appendix A and Appendix B.**

2.3 Consideration must be given, prior to authorisation as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of a human right is justified in the interests of the community as a whole, or whether the information could be gleaned in other ways.

2.4 A public authority may only engage the Act when in performance of its core functions, that is the specific public functions undertaken by the authority in contrast to the ordinary functions that are undertaken by every authority, for example, employment issues, contractual arrangements, etc.

3. Scrutiny and Tribunal

3.1 External Scrutiny

3.1.1 The Office of Surveillance Commissioners (OSC) was set up to monitor compliance with the Act. The OSC has "a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of the Act", and the Surveillance Commissioner will from time to time inspect the Council's records and procedures for this purpose.

3.1.2 In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g. directed surveillance. Applications will be heard on a judicial review basis. Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.

3.1.3 The Tribunal can order:

- Quashing or cancellation of any warrant or authorisation
- Destruction of any records or information obtained by using a warrant or Authorisation
- Destruction of records or information held by a public authority in relation to any person

3.1.4 The Council has a duty to disclose to the tribunal all documents they require if any Council officer has:

- Granted any authorisation under the Act
- Engaged in any conduct as a result of such authorisation

3.2 **Internal Scrutiny**

3.2.1 The Head of Legal & Democratic Services is responsible for:

- The integrity of the process in place within the Council to authorise directed surveillance and CHIS
- Compliance with Part II of the Act and with the accompanying Codes of Practice
- Engagement with the OSC when they conduct their inspections and
- Where necessary oversee the implementation of any post-inspection action plans recommended or approved by the OSC

3.2.2 The Overview and Scrutiny Committee will review the authority's use of the Act and the Policy and Guidance document at least once a year. They will also consider internal reports on the use of the Act on at least a quarterly basis to ensure that it is being used consistently with this Policy and that that Policy is fit for purpose. The Members will not, however, be involved in making decisions on specific authorisations.

4. Benefits of RIPA authorisations

4.1 The Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it will be lawful for all purposes. Consequently, the Act provides a ~~defence to an accusation of an infringement of a human right~~statutory framework under which covert surveillance can be authorised and conducted compatibly with Article 8 of the Human Rights Act 1998 – a person's right to respect for their private and family life, home and correspondence.

4.2 Material obtained through properly authorised covert surveillance is admissible evidence in criminal proceedings.

4.3 Section 78 Police and Criminal Evidence Act 1984 allows for the exclusion of evidence if it appears to the court that, having regard to all the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse affect on the fairness of the proceedings that the court ought not to admit it. Evidence obtained through covert surveillance will not be excluded unless the test of unfairness is met.

5. Definitions

5.1 'Covert' is defined as surveillance carried out in such a manner that is calculated to ensure that the person subject to it is unaware that it is or may be taking place. (s.26 (9)(a) of the Act)

5.2 'Covert human intelligence source' (CHIS) is defined as a person who establishes or maintains a relationship with a person for the covert process of obtaining information about that person. (s.26 (8) of the Act)

5.3 'Directed surveillance' is defined as covert but not intrusive and undertaken:

- for a specific investigation or operations
- in such a way that is likely to result in the obtaining of private information about any person
- other than by way of an immediate response (s.26 (2) of the Act)

5.4 'Private information' includes information relating to a person's private or family life.

5.5 'Intrusive' surveillance is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or using a surveillance device. **South Derbyshire District Council may not authorise such surveillance**.

5.6 'Authorising Officers' will be responsible to ensure their relevant members of staff are suitably trained as 'Applicants' so as to avoid errors in the operation of the process and completion of relevant forms. It is important that relevant Directors, Heads of Service and Authorised Officers take personal responsibility for the efficient and effective operation of this Policy and Guidance document within their respective areas.

5.7 Authorised Officers will also ensure that staff who report to them follow this Policy and Guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

5.8 Authorised Officers must also ensure when sending copies of any forms to the Head of Legal & Democratic Services, that they are sent in sealed envelopes marked 'RIPA – Private and Confidential'.

6. When does the Act apply ?

6.1 Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS is necessary for the purpose of preventing or detecting crime or of preventing disorder.

The Act does:

- require prior authorisation of directed surveillance
- prohibit the Council from carrying out intrusive surveillance
- require authorisation of the conduct and use of a CHIS
- require safeguards for the conduct and use of CHIS
- permit the Council to acquire communications data in certain circumstances

The Act does not:

- make unlawful conduct which is otherwise lawful
- prejudice or dis-apply any existing powers available to the District Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the District Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

6.2 If the Authorising Officer or any Applicant is in doubt, s/he should speak to a representative from the Legal Services Section BEFORE authorising, renewing, cancelling or rejecting any directed surveillance, use of a CHIS and/or acquisition of communications data.

CCTV

6.3 The normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV covertly and in a pre-planned manner as part of the specific investigation or operation to target a specific individual or group of individuals. Equally a request, say by the police, to track particular individuals via CCTV recordings may require authorisation (from the police).

7. Covert Human Intelligence Source ("CHIS")

7.1 Put simply, this means the use of "agent provocateur", undercover officers who do not reveal their true identity or professional witnesses used to obtain information and evidence.

7.2 The Act defines a CHIS under section 26 of the Act as anyone who:

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

(b) covertly uses such a relationship to obtain information or provide access to any information to another person; or

(c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

7.3 Any reference to the conduct of a CHIS includes the conduct of a source which falls within (a) to (c) or is incidental to it.

7.4 References to the use of a CHIS are references to inducing, asking or assisting a person to engage in such conduct.

7.5 Section 26(9) of the Act goes on to define:-

(b) a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose; and

(c) a relationship is used covertly, and information obtained as mentioned in paragraph 7(c) above and is disclosed covertly, if, and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

7.6 Juvenile Sources

7.6.1 Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under the age of 16 years be authorised to give information against his parents or any person who has parental responsibility of him. The duration of a juvenile CHIS is **one** month. The Regulation of Investigatory Powers (Juveniles) Order 2000 SI No. 2793 contains special provisions which must be adhered to in respect of juvenile sources.

7.7 Vulnerable Individuals

7.7.1 A vulnerable individual is a person who is, or may be, in need of community care services by reason of mental or other disability, age or illness and who is, or may be, unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances.

8. Types of Surveillance

8.1 '**Surveillance**' includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications
- recording anything mentioned above in the course of authorised surveillance
- surveillance, by or with, the assistance of appropriate surveillance device(s)

Surveillance can be overt or covert

8.2 **Overt Surveillance**

8.2.1 Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public and/or will be going about Council business openly.

8.2.2 Similarly, surveillance will be overt if the subject has been informed it will be happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.

8.3 **Covert Surveillance**

8.3.1 Covert surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place *(Section 26(9)(a) of the Act)*.

8.3.2 The Act regulates two types of covert surveillance, (directed surveillance and intrusive surveillance) and the use of Covert Human Intelligence Sources (CHIS's).

8.4 **Directed Surveillance**

8.4.1 Directed Surveillance is surveillance which: -

- is covert; and
- is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance);
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- it is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an

individual (whether or not that person is specifically targeted for purposes of an investigation), *(Section 26(10) of the Act).*

8.4.2 Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

8.4.3 Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private life of others.

8.4.4 **For the avoidance of doubt, only those Officers designated and certified to be 'Authorised Officers' for the purpose of the Act can authorise 'Directed Surveillance' IF, AND ONLY IF, the Act authorisation procedures detailed in this document ~~from *(insert date),*~~ are followed. If an Officer has not been 'authorised' for the purposes of the Act, s/he can NOT carry out or approve/reject any action set out in this policy and guidance document.**

8.5 **Intrusive Surveillance**

8.5.1 This is when it: -

- is covert;
- relates to residential premises and private vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premise will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

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

8.6 Proportionality

8.6.1 The term incorporates three concepts:

- the means should not be excessive in relation to the gravity of the mischief being investigated;
- the least intrusive means of surveillance should be chosen; and

- collateral intrusion involves invasion of third parties privacy and should, so far as is possible, be minimised.

8.6.2 Extra care should be taken over any publication of the product of the surveillance.

9. Authorisations (See flowchart at Appendix C)

9.1 Applications for directed surveillance

9.1.1 All application forms (**see Appendix D**) must be fully completed with the required details to enable the Authorising Officer to make an informed decision. The description of the proposed operation should be full and detailed, specifying any equipment to be used. The use of maps or sketches to show for example observation posts and target premises should also be considered.

No authorisation shall be granted unless the Authorising Officer is satisfied that the investigation is:

- necessary for one of the reasons listed above
- proportionate to the ultimate objective
- at an appropriate level (i.e. not excessive)

and that no other form of investigation would be appropriate.

The grant of authorisation should indicate that consideration has been given to the above points. The Authorising Officer's statement should include a full account of what is being authorised and how and why the Authorising Officer is satisfied that the operation is necessary and proportionate. The Authorising Officers statement should spell out the 'five W's'; whom the surveillance is directed against, what surveillance activity/equipment is sanctioned, when and where it will take place, and why it is necessary.

The Authorising Officer's statement should be completed in handwriting as a personal contemporaneous record of the thinking which justified the authorisation.

Necessity: Covert surveillance cannot be said to be necessary if the desired information can reasonably be obtained by overt means. It must also be necessary for the purpose of preventing or detecting crime or of preventing disorder.

Proportionality: The method of surveillance proposed must not be excessive in relation to the seriousness of the matter under investigation. It must be the method which is the least invasive of the target's privacy.
Proportionality should be carefully explained, not merely asserted, nor is describing parts of the operation itself germane to proportionality. A good explanation should refer to three elements:

1. balance the extent of the problem against the size and scope of the operation, demonstrating that it is not the proverbial 'sledgehammer to crack a nut';
2. explain that intrusion is to be kept to a minimum; and
3. show that having considered all other practical courses there is no other way in which the necessary evidence can be obtained (i.e. a covert operation is the last resort).

Collateral intrusion, which affects the privacy rights of innocent members of the public, must be minimised and use of the product of the surveillance carefully controlled so as to respect those rights.

Advice should be sought from the Legal & Democratic Services Section on any issues of concern.

9.1.2 The Authorising Officer must also take into account the risk of **'collateral intrusion'** i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation~~, particularly where there are special sensitivities e.g. premises used by lawyers, doctors or priests~~ e.g. ~~for any form of medical or professional counselling or therapy~~. The application must include an assessment of any risk of collateral intrusion for this purpose.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion.

Those carrying out the investigation must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent.

Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.

9.1.3 **Special consideration in respect of confidential information**

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved.

Confidential information consists of matters subject to legal privilege, communication between a Member of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material.
(ss 98-100 Police Act 1997)

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal

advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Head of Legal & Democratic Services should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's **spiritual welfare** or matters of **medical or journalistic confidentiality**.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under the Act may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive, or, in his absence, a member of Corporate Management Team and should only be authorised where there are exceptional and compelling circumstances that make the authorisation necessary.

9.1.4 Authorisations must be in writing except in urgent cases but these should be followed up in writing as soon as possible. Urgency only arises where to await written authorisation would endanger life or jeopardise the operation. Delay caused in obtaining an authorisation cannot justify an urgent, oral authorisation.

9.1.5 **Notifications to Inspector/Commissioner**

The following situations must be brought to the inspector/commissioner's attention at the next inspection:

- Where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved.
- Where a lawyer is the subject of an investigation or operation;
- Where confidential personal information or confidential journalistic information has been acquired and retained.

9.1.6 **Applications for CHIS**

Same as for directed surveillance except that the authorisation must specify the activities and identity of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

There are additional requirements in s29(5) of the Act relating to responsibility for dealing with the source and maintenance of records relating to the source.

All application forms (**see Appendix E**) must be fully completed with the required details to enable the Authorising Officer to make an informed decision.

In addition to the requirements of the Act the duties set out in the Source Records Regulations (S.I.2000/2725) must also be observed.

10. Working With/Through Other Agencies

When some other agency has been instructed on behalf of the Council to undertake any action under the Act, this document must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. Police, Customs & Excise, Inland Revenue, etc.):-

(a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Head of Legal & Democratic Services for the RIPA Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

(b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation, In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

In terms of 2(a), if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use. Copies of letters should be sent to the Head of Legal & Democratic Services for retention.

11. Duration and Cancellation

- An authorisation for **directed surveillance** shall cease to have effect (if not renewed) 3 months from the date of grant or renewal.

- An authorisation for **CHIS** shall cease to have effect (unless renewed) 12 months from the date of grant or renewal.

- An **oral** authorisation or renewal shall cease to have effect (unless renewed) 72 hours from the date of grant or renewal

This does not mean that the authorisation should be given for the whole period so that it lapses at the end of this time. The Authosing Officer, in accordance with s.45 of the Act, must cancel each authorisation as soon as the Authorising Officer decides that the surveillance should be discontinued. Authorisations should be for the minimum period reasonable for the purpose they are given and in any event will not last longer than 3 months.

Documentation of any instruction to cease surveillance should be retained and kept with the cancellation form.

12. Reviews

The Authorising Officer should review all authorisations at intervals determined by him/herself. This should be as often as necessary and practicable. **The reviews should be recorded.** If it is anticipated that the surveillance period will be short, an early review should be carried out and the authorisation subsequently cancelled.

If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these individuals. It would be appropriate to call a review specifically for this purpose.

Particular attention should be paid to the possibility of obtaining confidential information.

13. Renewals

Any Authorised Officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect.

A CHIS authorisation must be thoroughly reviewed before it is renewed.

14. Central Register of Authorisations

14.1 All authorities must maintain the following documents:

- Copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorised Officer;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the Authorising Officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation and supporting documentation submitted when the renewal was requested;
- The date and time when any instruction to cease surveillance was given
- The date and time when any other instruction was given by the Authorising Officer.

14.2 To comply with paragraph 14.1 above, the Head of Legal & Democratic Services holds the central register of all authorisations issued by officers of South Derbyshire District Council. A copy of every authorisation, renewal and cancellation issued should be lodged within 2 working days with the Head of Legal & Democratic Services in an envelope marked 'Private and Confidential'.

14.3 The Council must also maintain a centrally retrievable record of the following information:

- type of authorisation
- date the authorisation was given
- name and rank/grade of the Authorising Officer
- unique reference number of the investigation/operation
- title (including brief description and names of the subjects) of the investigation/operation;
- whether urgency provisions were used, & if so why
- details of renewal
- whether the investigation/operation is likely to result in obtaining confidential information
- whether the authorisation was granted by an individual directly involved in the investigation

- date of cancellation

These records will be retained for at least 3 years and will be available for inspection by the OSC.

15. Retention of records

~~All documents must be treated as strictly confidential and the~~ Authorising ~~Officer must make appropriate arrangements for their retention, security and destruction, in accordance with the Council's Data Protection Policy and the RIPA codes of practice. The retention period for the purposes of this guidance is three years from the ending of the period authorised.~~
The Authority must ensure that arrangements are in place for the secure handling, storage and destruction of materials obtained through the use of directed surveillance. The Authorising Officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice relating to the handling and storage of material.

The Central Register of Authorisations will be kept securely in a locked cabinet in the Legal & Democratic Services Department.

16. Complaints procedure

16.1 The Council will maintain the standards set out in this guidance and the Codes of Practice (**See Appendices A and B**). The Chief Surveillance Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by the Act.

16.2 Contravention of the Data Protection Act 1998 may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of this Policy and Guidance document should be made using the Council's own internal complaints procedure. To request a complaints form, please contact the Complaints Officer, South Derbyshire District Council, Civic Offices, Civic Way, Swadlincote, Derbyshire, DE11 0AH or telephone 01283 595784.

REGULATION OF INVESTIGATORY POWERS ACT 2000

GUIDANCE – PART II

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

Introduction

With effect from 5 January 2004, and in accordance with Chapter I of Part I of Regulation of Investigatory Powers Act ('the Act'), local authorities can authorise the acquisition and disclosure of 'communications data' provided that the acquisition of such data is necessary for the purpose of **preventing or detecting crime or preventing disorder**; and proportionate to what is sought to be achieved by acquiring such data

There is a [revised draft] Code of Practice **(Appendix F**) ('the Code')

NOTHING IN THIS CODE PERMITS THE INTERCEPTION OF THE CONTENT OF ANY COMMUNICATION.

The procedure is similar to that of authorisation for directed surveillance and CHIS but has extra provisions and processes.

The purpose and effect of the procedure is the same i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge.

The Authorising Officer is called a 'designated person'.

1. What is 'Communications data'?

Communications data is information relating to the use of a communications service e.g. postal service or telecommunications system. It is defined by Section 21(4) of the Act and falls into three main categories: -

Traffic data - where a communication was made from, to whom and when

Service data – use made of service e.g. Itemised telephone records

Subscriber data – information held or obtained by operator on person they provide a service to.

Local authorities are restricted to subscriber and service use data and only for the purpose of preventing or detecting crime or preventing disorder.

2. Designated person

A Designated Person must be at least the level of Unit Manager.

3. Application forms

All applications must be made on a standard form (**Appendix G)** and submitted to the single point of contact ("SPOC"). The SPOC will ensure that the application meets the required criteria and then pass to the Designated Person.

4. Authorisations

Authorisations can only authorise conduct to which Chapter II of Part I of the Act applies.

In order to comply with the Code, a Designated Person can only authorise the obtaining and disclosure of communications data if:

(i) it is **necessary** for any of the purposes set out in Section 22(2) of the Act. (NB South Derbyshire District Council can only authorise for the purpose set out in Section 22 (2) (b) which is the purpose of preventing or detecting crime or preventing disorder); and

(ii) it is **proportionate** to what is sought to be achieved by the acquisition of such data (in accordance with Section 22(5) of the Act)

Consideration must also be given to the possibility of collateral intrusion and whether any urgent timescale is justified.

Once a Designated Person has decided to grant an authorisation or a notice given there are two methods: -

(1) By authorisation of some person in the same relevant public authority as the designated person, whereby the relevant public authority collects the data itself (Section 22(3) of the Act). This may be appropriate in the following circumstances:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data.
- It is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

(2) By notice to the holder of the data to be acquired (Section 22(4) of the Act) which requires the operator to collect or retrieve the data. Disclosure may only be required to either the Designated Person or the single point of contact.

Service provider must comply with the notice if it is reasonably practicable to do so (s.22 (6)-(8) of the Act) and can be enforced to do so by civil proceedings.

The postal or telecommunications service can charge for providing this information.

There are standard forms (**Appendix G**) for authorisations and notice.

5. Oral authority

South Derbyshire District Council is not permitted to apply or approve orally.

6. Single point of contact ("SPOC")

Notices and authorisations should be passed through a single point of contact within the Council. This should make the system operate more efficiently as the SPOC will deal with the postal or telecommunications operator on a regular basis and also be in a position to advise a designated person on the appropriateness of an authorisation or notice.

SPOCs should be in position to:

- Where appropriate, assess whether access to communication data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and Designated Person on whether communications data falls under section 21(4)(a), (b) or (c) of the Act;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

A SPOC must be accredited which involves undertaking appropriate training.

7. Duration

Authorisations and notices are only valid for one month beginning with the date on which the authorisation is granted or the notice given. A shorter period should be specified if possible.

8. Renewal and cancellation

An authorisation or notice may be renewed at any time during the month it is valid using the same procedure as used in the original application. A renewal takes effect on the date which the authorisation or notice it is renewing expires.

The code requires that all authorisations and notices should be cancelled by the Designated Person who issued it as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The relevant postal or telecommunications operator should be informed of the cancellation of a notice.

9. Retention of records

Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner (see paragraph 10).

Applications must also be retained to allow the Tribunal (see paragraph 10 below) to carry out its functions.

A record must be kept of:-

- the dates on which the authorisation or notice is started or cancelled.
- any errors that have occurred in the granting of authorisations or giving of notices.

A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable.

Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the Data Protection Act 1998 must be observed.

The Head of Legal & Democratic Services will maintain a centrally retrievable register.

10. Oversight and Complaints

The Act provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained in Part I and the Code requires any person who uses the powers conferred by Part II to comply with any request made by the Commissioner to provide any information he requires to enable him to discharge his functions.

The Act also establishes an independent Tribunal to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure should be available for reference at South Derbyshire District Council's public offices.

APPENDIX A

Code of Practice

Covert Surveillance

See Home Office website:

~~http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/covert-cop?view=Binary~~

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-surveil-prop-inter-COP

APPENDIX B

Code of Practice

Covert Human Intelligence ~~Human Intelligence~~ Sources (CHIS)

See Home Office website:

~~http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/human-cop?view=Binary~~

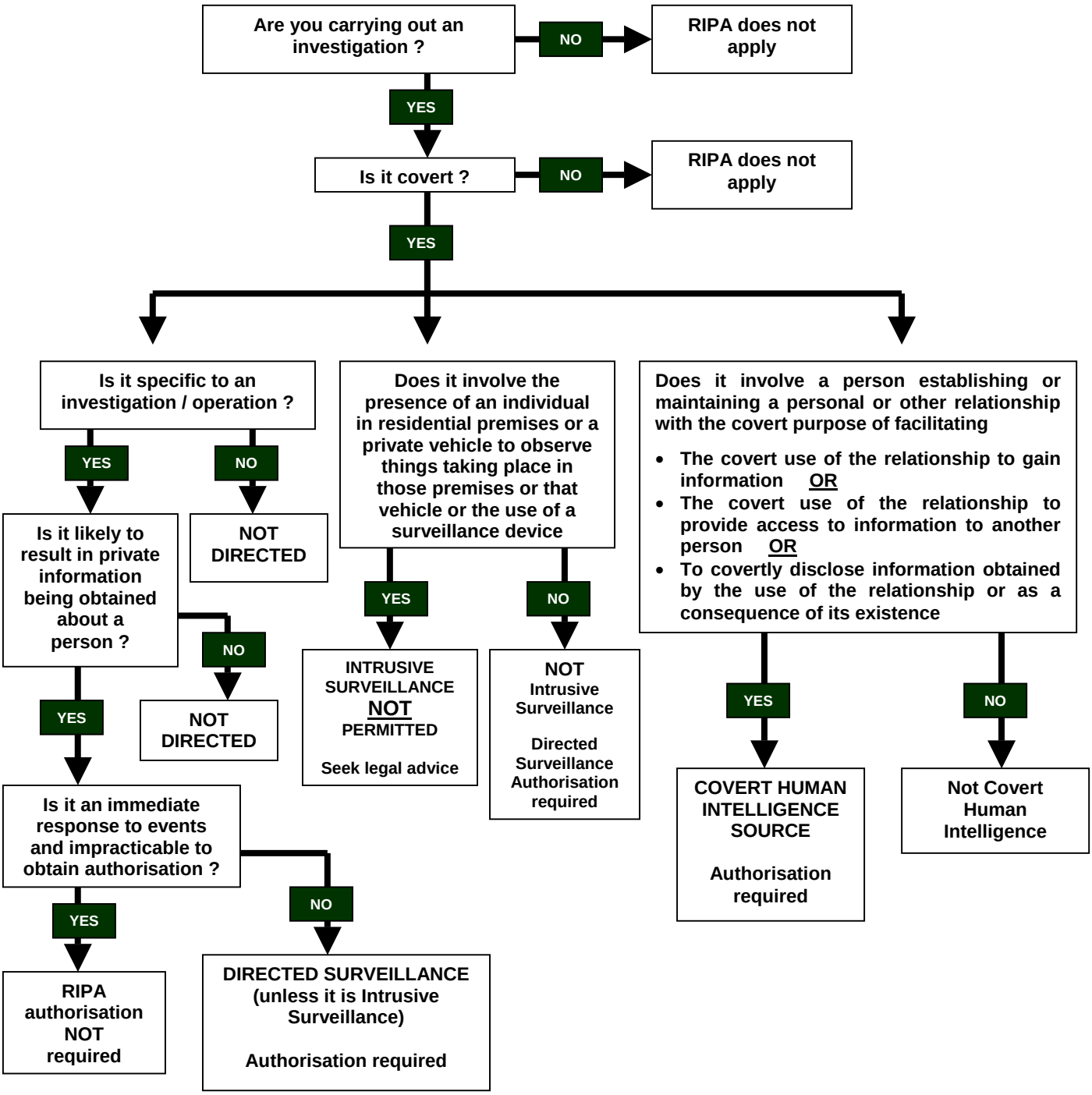
http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-human-intel-source-COP

APPENDIX C

DIRECTED SURVEILLANCE

Regulation of Investigatory Powers Act 2000

Do you need Authorisation ?



APPENDIX D

Forms

Directed Surveillance

APPLICATION

~~www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/application-directed-surveillanc?view=Standard&pubID=447375~~

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/application-directed-surveillanc?view=Standard&pubID=690596

REVIEW

~~www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/review-directed-surveillance?view=Standard&pubID=447381~~

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/review-directed-surveillance?view=Standard&pubID=690602

CANCELLATION

~~www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/cancellation-directed-surveillan?view=Standard&pubID=447377~~

Please note: As the Home Office website does not contain the latest version of the cancellation form, this is attached separately to this document at Appendix H

RENEWAL

~~www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/renewal-directed-surveillance?view=Standard&pubID=447379~~

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/renewal-directed-surveillance?view=Standard&pubID=690600

APPENDIX E

Forms

Covert Human Intelligence Sources (CHIS)

APPLICATION
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-application?view=Standard&pubID=447389

REVIEW
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-review?view=Standard&pubID=447372

CANCELLATION
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-cancellation?view=Standard&pubID=447391

RENEWAL
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-renewal?view=Standard&pubID=447370

APPENDIX F

Code of Practice

Acquisition and Disclosure of Communications data

See Home Office website:

~~http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf?view=Binary~~

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/acquisition-disclosure-cop

APPENDIX G

Forms – Part I

Communications data

APPLICATION
http://www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/communications-data.doc?view=Standard&pubID=446995

NOTICE TO COMMUNICATION SERVICE PROVIDER
www.security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/ripa-section-22-notice-update?view=Standard&pubID=590984

APPENDIX H

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

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

Details of cancellation:

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

Unique Reference Number	

2. Explain the value of the directed surveillance in the operation:

3. What product has been obtained as a result of the surveillance activity? (You should list here the dates and times of the activity; the nature of the product (i.e., what it shows) and its format (e.g., visual recordings; stills images); associated log/reference numbers; where the product is to be held; and the name of the officer responsible for its future management.) ***nb*** *– if you have already provided these details in earlier reviews, a cross-reference here should suffice.*

Dates/times	Product obtained	Format & reference numbers	Storage location	Officer responsible

Name (Print) ---------- **Grade** ----------

Signature ---------- **Date** ----------

4. Authorising Officer's comments on product obtained. (Paragraph 2.18 of the Covert Surveillance Code of Practice states that arrangements must be in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material. **You should record here how you intend this to be achieved**.)

Unique Reference Number	

5. Authorising Officer's comments on the outcome of this use of directed surveillance and formal cancellation instructions.			
Name (Print)	----------	**Grade**	----------
Signature	----------	**Date and Time**	----------

6. Time and Date when the Authorising Officer instructed the surveillance to cease *(if done verbally prior to this formal written cancellation)*.			
Date:		**Time:**	