SOUTH DERBYSHIRE DISTRICT COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

POLICY AND GUIDANCE

CONTENTS

Page nos.

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

All applications for authorisation in accordance with RIPA ('Authorising Officers') will be considered by a member of the Corporate Management Team identified in the table below (Chief Executive, Director of Finance and Corporate Services, Director of Housing and Environmental Services). Any incomplete or inadequate application forms will be returned to the applicant for amendment. Authorising Officers 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 Legal and Democratic Services Manager for entry on the Central Register.

AUTHORISING OFFICERS
CHIEF EXECUTIVE
DIRECTOR OF FINANCE & CORPORATE SERVICES
DIRECTOR OF HOUSING & ENVIRONMENTAL SERVICES

Senior Responsible Officer

The Senior Responsible Officer is the Chief Executive. The Senior Responsible Officer has overall responsibility for RIPA, as outlined in the Codes of Practice and the Council's Policy and Guidance.

RIPA Co-ordinating Officer / Training

The RIPA Co-ordinating Officer is the Council's Legal and Democratic Services Manager. The RIPA Co-ordinating Officer is responsible for the maintenance of the Central Record of Authorisations and the collation of RIPA applications/authorisations, reviews, renewals, and cancellations. In addition, there is responsibility for providing oversight of the RIPA process within the Council and for RIPA training.

The RIPA Co-ordinating Officer shall ensure that refresher training is offered once a year to all directorates of the Council and also give advice and training on request.

The RIPA Co-ordinating Officer is responsible for raising RIPA awareness within the Council.

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

Legislative Changes

By virtue of sections 37 and 38 of the Protection of Freedoms Act 2012, from 1st November 2012 the Council will be required to obtain judicial approval prior to using covert techniques. Authorisations and notices under RIPA will only be given effect once an Order has been granted by a Justice of the Peace (JP), a District Judge or lay Magistrate.

Local authorities in England and Wales can no longer seek the protection of the Act on the grounds provided by subsections 28(3)(d) and (e) (i.e. in the interests of public safety and for the purpose of protecting public health). In relation to directed surveillance (though not to authorising CHIS), their remaining powers were further limited by Statutory Instrument 2012/1500. To authorise directed surveillance, the Authorising Officer must demonstrate that the proposed activity is necessary for the prevention or detection of a crime which either carries a maximum sentence of at least six months' imprisonment or is an offence relating to the sale of alcohol or tobacco products to minors. (As to the definition of 'detecting crime', see RIPA section 81(5).) [Note 78 OSC's 2014 Procedures and Guidance document].

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 Authorising Officers 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 is also a Code of Practice in relation to the use of these powers and this attached at **Appendix A.** Attached at **Appendix C** is reference to the Procedure and Guidance document issued by the Office of Surveillance Commissioners in December 2014.

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 Senior Responsible Officer 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.

Elected Members and Senior Responsible Officers (see paragraphs 3.27 and 9.2 of the CHIS Code of Practice) are required to ensure that policies are fit for purpose and that Authorising Officers are competent. An Elected Member has no need to know the identity of a CHIS nor know the detail of conduct authorisations. Chief Executives may provide Elected Members

with a copy of OSC inspection reports, redacted if necessary. [Note 251 OSC's 2014 Procedures and Guidance document].

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 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 and can embrace aspects of business and professional 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 Authorising Officers take personal responsibility for the efficient and effective operation of this Policy and Guidance document within their respective areas.

5.7 Authorising 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 Authorising Officers must also ensure when sending copies of any forms to the RIPA Co-ordinating Officer, 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 Authorising Officers or any Applicants are 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 is 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.

A local authority may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed (see CHIS Code of Practice 6.12). In the absence of such an agreement the local authority must be capable of fulfilling its statutory responsibilities. [Note 250 OSC's 2014 Procedures and Guidance document].

Some local authorities may not wish to use CHIS and may in practice avoid authorising CHIS. However, all such local authorities should

recognise that the occasion may arise when a CHIS appears unexpectedly and has to be authorised and managed. Consequently all local authorities must be equipped with a policy and awareness training to recognise status drift. [Note 252 OSC's 2014 Procedures and Guidance document].

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.

Only the Chief Executive, or somebody deputising for him in his absence, may authorise the employment of juvenile sources, vulnerable individuals and the obtaining of confidential information.

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).*

Directed surveillance is covert surveillance that is carried out for the purposes of a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person, whether or not he is a subject of the action. It includes the activity of monitoring, observing, listening and recording by or with the assistance of surveillance equipment. It need not be subject specific. A search for an identified person in a public place will not amount to directed surveillance, unless it includes covert activity that may elicit private information about that person or any other person. Any processing of data (e.g. taking a photograph to put on record) is an invasion of privacy. [Note 269 OSC Procedures and Guidance 2010]

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 'Authorising Officers' for the purpose of the Act can authorise 'Directed Surveillance' IF, AND ONLY IF, the Act authorisation procedures detailed in this document 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 **Directed Surveillance Crime Threshold**

The crime threshold applies only to the authorisation of directed surveillance by the Council under RIPA, not to the authorisation of the Council's use of CHIS or the acquisition of communications data.

The amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 have the following effect:

- The Council can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol and tobacco.
- The Council cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months imprisonment.
- The Council may therefore continue to authorise the use of directed surveillance in more serious cases as long as the other tests are met, i.e. that it is necessary and proportionate and where approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of 6 months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.
- The Council may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted.

- The Council may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.

8.5.1 **Impact on Investigations**

At the start of an investigation, Officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use it must be clear that the threshold is met and that it is necessary and proportionate to use it.

During the course of an investigation the type and seriousness of offences may change. The option of authorising directed surveillance is dependent on the offence under investigation attracting a sentence of a maximum 6 months imprisonment or more or being related to the underage sale of alcohol and tobacco. Providing the offence under investigation is one which appears on the statute book with at least a maximum 6 months term of imprisonment or is related to the specific offences listed in the order concerning the underage sale of alcohol and tobacco an application can be made. However, if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold, the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

Directed surveillance will be authorised against a specific offence which meets the threshold, and the type and the timing of the deployment of the surveillance will always reflect this. There may be cases where it is possible, with the same evidence obtained by the same deployment, to substantiate a variety of different charges, some of which fall below the threshold, it will be for the Courts too decide whether to admit, and what weight to attach to, the evidence obtained in the lesser charges.

The Council will no longer be able to use directed surveillance in some cases where it was previously authorised. But this does not mean that it will no be possible to investigate these areas with a view to stopping offending behaviour. The statutory RIPA Code of Practice makes it clear that routine patrols, observation at trouble ‘hotspots’, immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

8.6 **Intrusive Surveillance**

8.6.1 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.

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

8.7 **Proportionality**

8.7.1 Proportionality is a key concept of the Act. If the activities are deemed necessary, the person granting the authorisation must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

8.7.2 The term incorporates four 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; and
- the activity must be proportionate to the degree of target on others.

8.7.3 When assessing proportionality, the following four elements of proportionality must be fully considered:

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
- explaining how and why the methods to be adopted will cause the least possible intrusion on the targets and others,
- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
- providing evidence of other methods considered and why they were not implemented. [Note 74.4 OSC's 2014 Procedures and Guidance document]

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

9. Authorisations (See flowchart at Appendix D)

9.1 **Applications for directed surveillance**

All application forms (**see Appendix F**) 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.

Section 32(5) of RIPA requires the Authorising Officers to describe and specify what he is granting. This may or not be the same as requested by the applicant. For the benefit of those operating under the terms of an authorisation, or any person who may subsequently review or inspect an authorisation, it is essential to produce, with clarity, a description of that which is being authorised (i.e. who, what, where, when and how). Authorising Officers should as a matter of routine state explicitly and in his own words what is being authorised, and against which subjects, property or location. Mere reference to the terms of the application is inadequate. [Note 116 OSC Procedures and Guidance 2010].

Authorising Officers must be careful in the use of 'or' and 'and' in order not to restrict what is intended. For example, do not use 'or' when 'and' is meant (e.g. deployment of ….on vehicle A or vehicle B' limits deployment to either vehicle, not both simultaneously or one after the other). [Note 118 OSC Procedures and Guidance 2010].

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

Authorising Officers should set out, in his own words, why he is satisfied or why he believes (RIPA) the activity is necessary and proportionate. A bare assertion is insufficient. [Note 75 OSC's 2014 Procedures and Guidance document].

9.1.1 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.

Authorising Officers must be satisfied that the use of covert surveillance is necessary for one of the purposes specified in section 28(3) of RIPA. In order to be satisfied, the conduct that it is aimed to prevent or detect must be identified and clearly described, particularly if it is questionable whether

serious crime criteria are met. Often missed is an explanation of why it is necessary to use the covert techniques requested. [Note 72 OSC's 2014 Procedures and Guidance document].

9.1.2 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 potential model answer would make clear that the four elements of proportionality had been fully considered:

1. balancing the size and scope of the operation against the gravity and extent of the perceived mischief;
2. explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
3. that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result; and
4. providing evidence of other methods considered and why they were not implemented. [Note 72 OSC's 2014 Procedures and Guidance document].

An authorisation should demonstrate how an authorising officer has reached the conclusion that the activity is proportionate to what it seeks to achieve, including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods but of explaining why the particular covert method, technique or tactic is least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. [Note 105 OSC Procedures and Guidance 2010]

The Authorising Officer should set out in his own words, why he believes the activity is necessary and proportionate. A bare assertion is insufficient. [Note 75 OSC's 2014 Procedures and Guidance document].

To assist an Authorising Officer to reach a proper judgment, the value of the date, information or intelligence on which the application has been made should be made clear. It is considered best practice for law enforcement agencies to utilise standard evaluation nomenclature which grades both the source and the information. While it is not necessary or desirable in the application to spell out in detail the content of intelligence logs, cross-referencing to these enables an Authorising Officer to check detail. Particular care should be taken when using date or information obtained from open or unevaluated sources such as the Internet or social networks. [Note 76 OSC's 2014 Procedures and Guidance document].

The law prevents an applicant or Authorising Officer from referring to interception and this presents significant difficulty when covert surveillance is to be based solely on that type of intelligence. Without product derived

from other acquisition methods, or an approved summary of the closed material, covert surveillance cannot be authorised. [Note 77 OSC's 2014 Procedures and Guidance document].

9.1.3 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.

This note applies to directed surveillance only. To comply with *R v Sutherland* the Authorising Officer should clearly set out what activity and surveillance equipment is authorised in order that those conducting the surveillance are clear on what has been sanctioned at each stage in the authorisation process. It is recognised that it is not always possible, at the outset of an investigation, to foresee how it will progress, but this should not provide a reason for the applicants to request a wide number of tactics 'just in case' they are later needed. The Authorising Officer may not authorise more than can be justified at the time of their decision and should demonstrate control and a proper understanding of necessity, collateral intrusion and proportionality, relating to each tactic requested. In straightforward cases, an applicant should request only the tactics that are known to be available and intended to be used. In more complex cases, where it is foreseen based on operational experience and assessed intelligence that additional tactics may be required as the investigation develops, additional tactics may be requested by way of review. The Authorising Officer should consider the use made of tactics to date, along with their impact and any product, to ensure that each additional tactic is necessary, whether collateral intrusion can be justified, and whether the cumulative effect of the tactics is proportionate in light of progress. Amendment must be explicit and no tactic may be used prior to it being granted by an Authorising Officer. OSC inspections will place significant emphasis on review and renewal procedures to ensure that Authorising Officers are addressing legal requirements throughout the life of an authorisation. [Note 98 OSC's 2014 Procedures and Guidance document].

It is unlikely to be regarded as 'not reasonably practicable' for an Authorising Officer to consider an application, unless he is too ill to give attention, on annual leave, is absent from his office and his home, or is for some reason not able within a reasonable time frame to obtain access to a secure telephone or fax machine. Pressure of work is not to be regarded as rendering it impracticable for Authorising Officers to consider an application. [Note 103 OSC's 2014 Procedures and Guidance document].

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

Authorising Officers 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. 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 Authorising Officers 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.

9.1.4 **The retention of applications with 'wet signatures'**

The key signature is that of the Authorising Officer on the authorisation. The only way it is possible to establish that the Authorising Officer has applied his own mind to the authorisation is it is handwritten by him. Typed documents are open to the suggestion that the authorisation is prepared by another and simply signed by the Authorising Officer. If information technology is used to construct applications and authorisations, it must be capable of authentication, hand-written (so-called 'wet') signatures are required to avoid accusation that the authorisation has been altered ex post facto. If an Authorising Officer relies on words prepared by another, his signature signifies responsibility for those words. Authorisations with wet signatures may be retained by the Authorising Officer or centrally, the latter being the preferred option. It is always open to a trial judge to require evidence which satisfies him that documents relied on are authentic. All public authorities must be ready to provide the relevant witness where authenticity is open to question. [Note 115 OSC's 2014 Procedures and Guidance document].

9.1.5 **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 RIPA Co-ordinating Officer 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 whoever deputises for him in his absence, and should only be authorised where there are exceptional and compelling circumstances that make the authorisation necessary.

9.1.6 **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.

9.1.7 **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 G**) must be fully completed with the required details to enable Authorising Officers to make an informed decision.

There should be a controller, a handler and recorder for a CHIS together with the requirement for a risk assessment if one is to be employed.

The handler will have day to day responsibility for:-

- dealing with the CHIS;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's welfare and security

The handler of a CHIS will usually be of a rank or position below that of the Authorising Officer.

The controller will normally be responsible for the management and supervision of the handler and general oversight of the CHIS.

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

Any officer considering applying for a CHIS should consult the RIPA Co-ordinating Officer before taking any practical steps.

10. Social Networking Sites (SNS) and Hotlines

The use of the internet may be required to gather information prior to and/or during an investigation, and this may amount to directed surveillance. Where there is an intention to use the internet as part of an investigation, consideration must be given as to whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation must be sought. Where an investigating Officer may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

- Officers must not create a false identity in order to 'friend' individuals on social networks.

- Officers viewing an individual's profile on a social network should do so only once in order to obtain evidence to support or refute their investigation.

- Further viewing of open profiles on social networks, to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a JP.

- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

Officers should also be aware of the risks of 'status drift' whereby a hotline informant, who initially supplies information in a manner not requiring authorisation, has developed inadvertently into a CHIS. In such a case CHIS relationship is formed invoking the procedures set out above.

The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same. [Note 288 OSC's 2014 Procedures and Guidance document].

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. repeat viewing of 'open source' sites may constitute directed surveillance on a case by case basis and this should be borne in mind. [Note 288.1 OSC's 2014 Procedures and Guidance document].

Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content). [Note 288.2 OSC's 2014 Procedures and Guidance document].

It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws. [Note 288.3 OSC's 2014 Procedures and Guidance document].

A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done. [Note 288.4 OSC's 2014 Procedures and Guidance document].

11. Judicial Approval

In order to authorise the use of directed surveillance, acquisition of communications data and use of a CHIS under RIPA, the Council will need to obtain an Order approving the grant or renewal of an authorisation from a JP before it can take effect. If the JP is satisfied that the statutory

tests have been met and that the use of the technique is necessary and proportionate he/she will issue an Order approving the grant or renewal for the use of the technique as described in the application.

Judicial approval is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an Authorising Officer remains the same.

11.1 **Procedure for Applying for Judicial Approval**

11.1.1 Making the Application

The flowchart at **Appendix E** outlines the procedure for applying for judicial approval. The application must be made by the Council. Following approval by the Authorising Officer the first stage of the process is for the local authority to contact Her Majesty's Courts and Tribunals Service administration team at the Magistrates Court to arrange a hearing.

The Council will need to provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and should contain all information that is relied upon. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his/her consideration.

The original RIPA authorisation or notice should be shown to the JP but will be retained by the Council so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigation by the Investigatory Powers Tribunal. The Court may wish to take a copy.

In addition, the Council will provide the JP with a partially completed judicial application/order form (**Appendix K**).

Although the Council is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

The order section of the form will be completed by the JP and will be the official record of the JP's decision. The Council will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and the Council will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

Legal Services will contact the Magistrates Court to arrange a hearing. On the rare occasions where out of hours access to a JP is required then it will be for Legal Services to make arrangements with Court legal staff.

11.1.2 Attending a Hearing

The hearing is a 'legal proceeding' and Council Officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.

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

The investigating/Authorising Officer will need to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. The investigating Officer will have detailed knowledge of the investigation and will have determined that use of a covert technique is required in order to progress a particular case. This does not, however, remove or reduce in any way the duty of the Authorising Officer to determine whether the tests of necessity and proportionality have been met, Similarly, it does not remove or reduce the need for the forms and supporting papers that the Authorising Officer has considered and which have been provided to the JP to make the case.

A Legal Officer will also be in attendance at court.

The Commissioners consider the best officer to apply to the magistrate for approval of an authorisation of directed surveillance or CHIS is the Authorising Officer, though they recognise this is not always possible. Only he can answer questions about his reasoning on necessity, proportionality, collateral intrusion and risk. [Note 291 of the OSC's 2014 Procedures and Guidance document]

If the Authorising Officer is not present before the magistrate, any comments made by the magistrate should be promptly reported to him. Such comments might affect the future conduct of the authorised activity, its duration and the regularity of reviews. A record should be made of such comments and of the action taken by the Authorising Officer to incorporate or address them. [Note 292 of the OSC's 2014 Procedures and Guidance document].

An authorisation of directed surveillance or CHIS does not take effect until it has been approved and signed by the magistrate. Local authorities should record the dates and times of signature by both the Authorising Officer and the magistrate. Care should be taken to record the expiry date accurately thereafter. [Note 293 of the OSC's 2014 Procedures and Guidance document].

Local authorities in England and Wales should also bear in mind that the power to make urgent oral authorisations has been removed, because section 43(1)(a) of RIPA no longer applices to authorisations requiring a magistrate's approval. All authorisations, even if urgent, must be made in writing, and local authorities'' RIPA policy documents should make this clear. [Note 294 of the OSC's 2014 Procedures and Guidance document].

11.1.3 Decision

The JP will consider whether he/she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that that the person who granted the authorisation or gave the notice was an appropriate designated person within the Council and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

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

If further information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refuse the Council should consider whether they can reapply, for example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

The JP will record his/her decision on the order section of the judicial application/order form. The Magistrates Court will retain a copy of the Councils RIPA authorisation or notice and the judicial application/order form. This information will be retained securely. Magistrates' Courts are not public authorities for the purposes of the Freedom of Information Act 2000.

The Council will need to provide a copy of the order to the communications Single Point of Contact for all communication data requests. Single Points of Contact must not acquire the communication data requested, until the JP has signed the order approving the grant.

11.1.4 Outcomes

Following consideration of the case the JP will complete the order section of the judicial application/order form recording their decision. The JP may decide to:

- Approve the Grant or renewal of an authorisation notice.
  The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case.
  In relation to communications data, the Council will be responsible for providing a copy of the Order or the Single Point of Contact.

- Refuse to approve the grant or renewal of an authorisation or notice.
  The RIPA authorisation or notice will not take effect and the Council may not use the technique in that case.
  Where an application has been refused the Council may wish to consider the reasons for refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those steps have been taken.

- Refuse to approve the grant or renewal and quash the authorisation or notice.
  This applies where a Magistrates Court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.
  The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of refusal in which to make representations.

11.1.5 Complaints/Judicial Review

There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates Advisory Committee.

The Council may only appeal a JP decision on a point of law by judicial review.

The Investigatory Powers Tribunal will continue to investigate complaints about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the Tribunal does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.

12. 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 RIPA Co-ordinating Officer 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 RIPA Co-ordinating Officer for retention.

13. 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.

If the proposed operation is expected to be completed quickly, then an early review should take place and Authorising Officers, in accordance with s.45 of the Act, must cancel each authorisation as soon as Authorising Officers decide that the surveillance should be discontinued.

It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. [Note 138 OSC Procedures and Guidance 2010].

The fact that the operation to which authorisation relates is only expected to last for a short time cannot affect the authorisation period. An early review can take care of issues of continuing necessity and proportionality. [Note 119 OSC Procedures and Guidance 2010].

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

When cancelling an authorisation, Authorising Officers should:

1. Record the time and date (if at all) that surveillance took place and the order to cease the activity was made.

2. The reason for cancellation.

3. Ensure that surveillance equipment has been removed and returned.

4. Provide directions for the management of the product.

5. Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.

6. Record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met). [Note 141 OSC Procedures and Guidance 2010].

A Surveillance Commissioner and Authorising Officers can only authorise on the basis of what they have been told. Issues of disclosure should not inhibit the proper construction of applications and authorisations but can be dealt with at the appropriate time using existing procedures. Where necessary, authorisations should cross-refer to the intelligence report. [Note 144 OSC Procedures and Guidance 2010].

To comply with *R V Sutherland* Authorising Officers should clearly set out what activity and surveillance equipment is authorised in order that those conducting the surveillance are clear on what has been sanctioned. [Note 145 OSC Procedures and Guidance 2010].

14. Reviews

Authorising Officers 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.

Reviews and renewals should not broaden the scope of the investigation but can reduce its terms. Where other subjects may unexpectedly come under surveillance, authorisations can anticipate it by using words such as 'suspected of', 'believed to be' or 'this authority is intended to include conversations between any and all of the subjects of this investigation, including those whose identities are not yet known'. [Note 125 OSC Procedures and Guidance 2010].

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

15. Renewals

Authorising Officers 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.

16. Central Register of Authorisations

16.1 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 Authorising Officers;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by Authorising Officers;
- 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 Authorising Officers.

16.2 To comply with paragraph 16.1 above, the RIPA Co-ordinating Officer 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 RIPA Co-ordinating Officer in an envelope marked 'Private and Confidential'.

16.3 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.

17. Retention of records

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 Services Section.

18. Complaints procedure

18.1 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.

18.2 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

Following implementation of sections 37 and 38 of the Protection of Freedoms Act 2012, from 1st November 2012 the acquisition of communications data will be subject to obtaining an Order approving the authorisation or notice from a JP.
(Please revert to the 'Judicial Approval' section of this document at page 18)

There is a Code of Practice **(Appendix** H **)** ('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 I)** 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 I**) 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 communications 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 RIPA Co-ordinating Officer 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

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interrefernce_web__2_.pdf

APPENDIX B

Code of Practice

Covert Human Intelligence Sources

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384976/Covert_Human_Intelligence_web.pdf

APPENDIX C

Office of Surveillance Commissioners

Procedures & Guidance 2014

Please note:

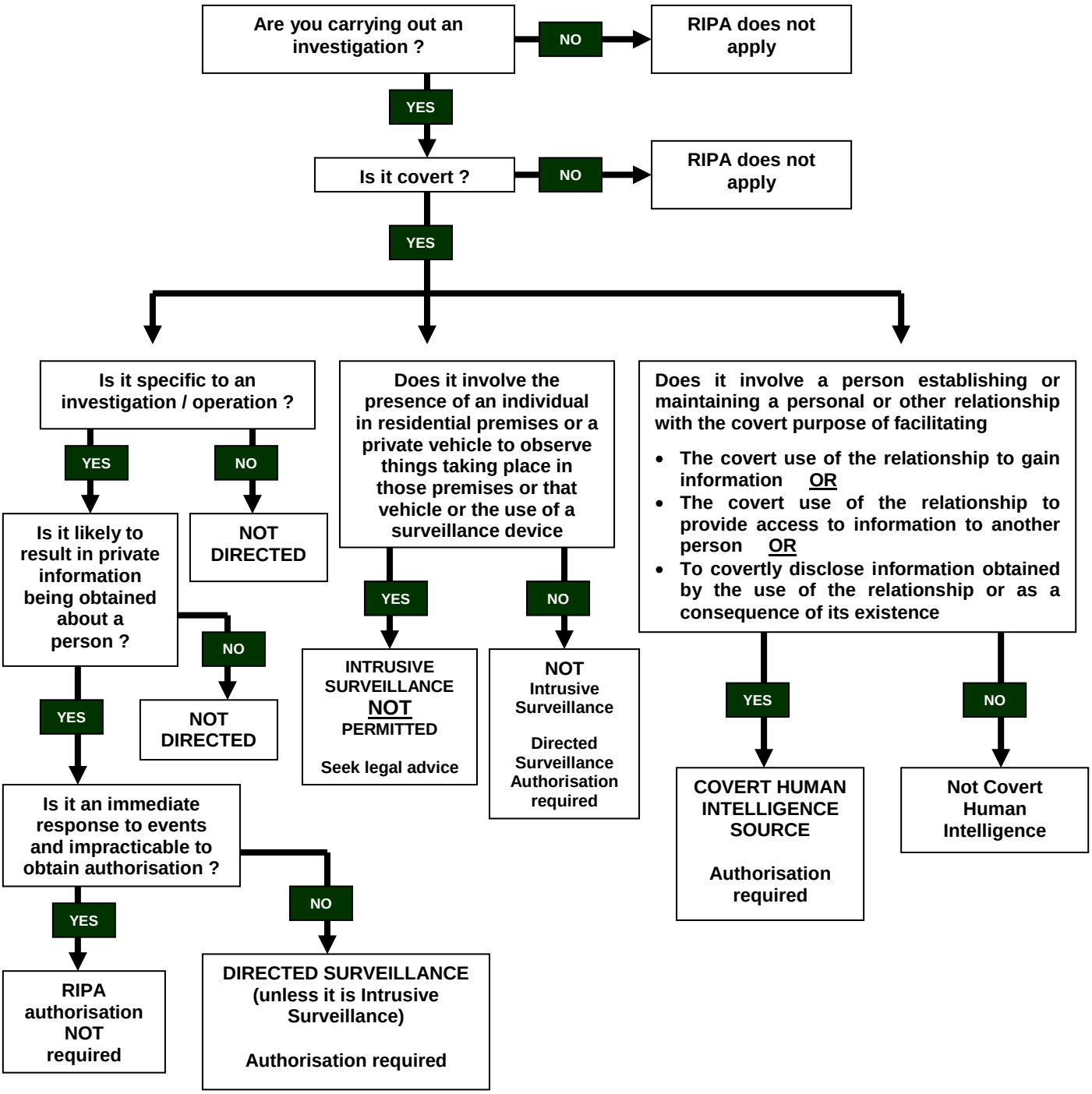
There is no link to this document on the Office of Surveillance Commissioners' website, it is available from Legal Services in hard copy

APPENDIX D

DIRECTED SURVEILLANCE

Regulation of Investigatory Powers Act 2000

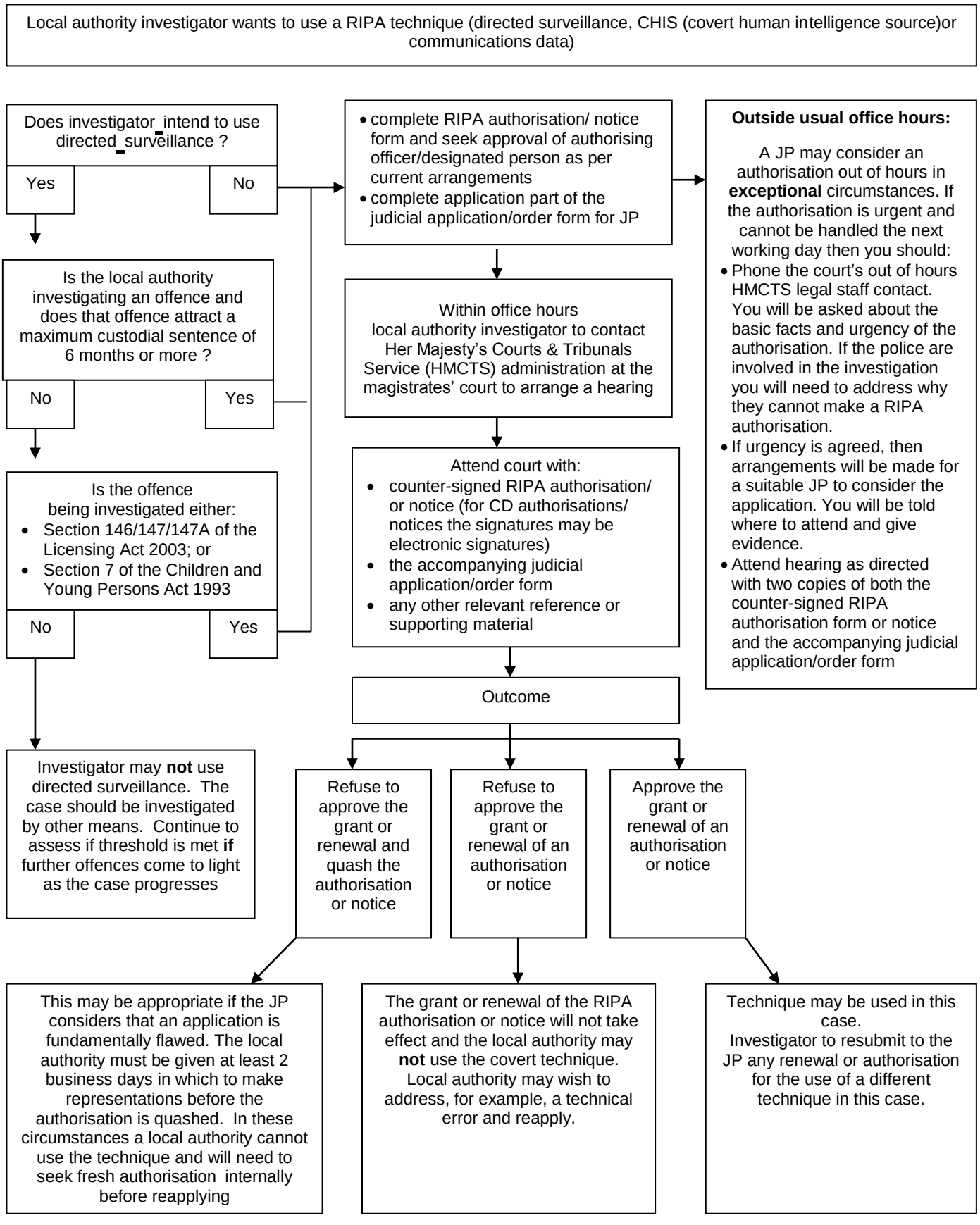
Do you need Authorisation ?



APPENDIX E

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER

TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



APPENDIX F

Forms

Directed Surveillance

APPLICATION

https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance

REVIEW

https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance

CANCELLATION

https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form

RENEWAL

https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance

APPENDIX G

Forms

Covert Human Intelligence Sources (CHIS)

APPLICATION

https://www.gov.uk/government/publications/application-for-the-use-of-covert-human-intelligence-sources-chis

REVIEW

https://www.gov.uk/government/publications/reviewing-the-use-of-covert-human-intelligence-sources-chis

CANCELLATION

https://www.gov.uk/government/publications/cancellation-of-covert-human-intelligence-sources-chis

RENEWAL

https://www.gov.uk/government/publications/renewal-of-authorisation-to-use-covert-human-intelligence-sources

APPENDIX H

Code of Practice

Acquisition and Disclosure of Communications data

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

APPENDIX I

Forms – Part I

Communications data

APPLICATION

https://www.gov.uk/government/publications/chapter-ii-application-for-communications-data

NOTICE TO COMMUNICATION SERVICE PROVIDER

https://www.gov.uk/government/publications/specimen-part-i-chapter-ii-notice

APPENDIX J

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

Local authority: ……

Local authority department: ……

Offence under investigation: ……..……..……..

Address of premises or identity of subject: ……..……..

……..……..

……..……..

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

……..……..

……..……..

……..……..

……..……..

……

……..……..

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

Investigating Officer: ……

Authorising Officer/Designated Person: ……

Officer(s) appearing before JP: ……..

Address of applicant department: ……..

……

Contact telephone number: ……

Contact email address (optional): ……..

Local authority reference: ……

Number of pages: ……

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

Magistrates' court: ……

Having considered the application, I (tick one):

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

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

……

……

……

……

……

Reasons

……

……

……

……

……

……

Signed:

Date:

Time:

Full Name:

Address of magistrates' court: