DERBY CITY COUNCIL

GUIDANCE TO STAFF ON SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORYPOWERS ACT 2000

Updated December 2014

CONTENTS

Chapter No **Page No.**

1.1 INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 ("the 2000 Act") regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to effectively discharge their investigatory functions.

1.2 The Council is included within the 2000 Act framework with regard to the authorisation of both Directed Surveillance and the use of Covert Human Intelligence Sources - Part I, Chapter I of the 2000 Act, as well as for the purposes of accessing relevant communications data under Part I, Chapter II of the 2000 Act.

1.3 The purpose of this guidance is to:

- explain the scope of the 2000 Act and the circumstances where it applies
- provide guidance on the authorisation procedures to be followed.

1.4 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and each department has copies of the codes to which staff can refer.

Overview

1.5 In summary, the 2000 Act requires that when the Council undertakes **directedsurveillance,** uses a***covert human intelligence source***(CHIS) or accesses **communications data** those activities must only be authorised by officers with sufficientmandate and training to do so, and who follow a defined set of processes in undertaking the functions of their roles.

1.6 For directed surveillance and CHIS operations, each department has nominated officers who can authorise both these activities. With the former,

the Councils Constitution delegates this function to three Service Directors, namely:

- Director of Customer Management
- Director of Younger Adults and Housing and
- Director of Environment and Regulatory Services

This is incorporated into the list at Appendix 3.

They are Service Directors for in-house services performing most of the statutory regulatory functions. All have received RIPA training.

1.7 For communications data purposes, a number of roles that tie in with the operating principles of the relevant Code of Practice are created within the Council for the administration of the processes involved. More details are contained in Chapter 6 of this document. The list of roles and identities of the officers occupying those roles is also contained in Appendix 3.

1.8 Authorisation under the 2000 Act gives lawful authority to carry out surveillance and the use of a source, and to acquire communications data. Obtaining authorisation or giving a Notice helps to protect the Council and its officers from complaints of interference with the right protected by Article 8(1) of the European Convention on Human Rights which is now enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be in accordance with the law. Provided the activities undertaken are also **necessary** and **proportionate** they will not be in contravention of Human Rights legislation.

1.9 **It should be noted that the Council <u>cannot</u> authorise intrusive surveillance**. Intrusivesurveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, that involves the presence of an individual on the premises or in the vehicle, or is carried out by a means of a surveillance device. Investigators should therefore be aware that any proposed form of surveillance that may involve interfering with an individual's property rights, and/or with wireless telegraphy, would be unlawful. Urgent advice should be sought from the Council's Legal Services Team in the event that the absence of surveillance

evidence could have a prejudicial effect on ongoing investigations.

1.10 Investigators should familiarise themselves with the provision of sections 4 and 5 of the Code of Practice on Directed Surveillance to ensure a good understanding of the limitation of powers within the 2000 Act.

1.11 Deciding when authorisation is required involves making a judgement. For example, environmental health officers might covertly observe and then visit a shop as part of their enforcement functions. Such observations may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras. Where this does not involve systematic surveillance of an individual, it forms a part of the everyday functions of law enforcement. This low-level activity will not usually be regulated under the provisions of the 2000 Act. Conversely where systematic covert surveillance is undertaken then an authorisation will be required.

1.12 The 2000 Act and the relevant codes of practice do not apply to the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use in Council buildings to prevent crime, and in several open places around the city. If you are in doubt about whether the nature of surveillance falls within the scope of the 2000 Act, seek the advice of an Authorising Officer. If they are in doubt they will seek legal advice.

The Benefits of Obtaining Authorisations

1.13 For both surveillance and the use of covert human intelligence sources, the 2000 Act states that:

- if an authorisation confers entitlement to engage in certain conduct, and
- the conduct is in accordance with the authorisation, then
- it should be *"lawful for all purposes"*.

1.14 The 2000 Act states that a person shall not be subject to any civil liability in relation to any conduct of his which:

a) is incidental to any conduct that is lawful by virtue of section 27(1); and
is not itself conduct an authorisation or warrant for which is capable of

being granted under a relevant enactment and might reasonably have been expected to have been sought in the case in question.

2. DIRECTED SURVEILLANCE

What Is Meant By Surveillance?

2.1 Surveillance includes:

a) monitoring, observing or listening to persons, their movement, their conversations or their other activities or communication

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device.

When Is Surveillance Directed?

2.2 Surveillance is directed for the purposes of the 2000 Act if it is covert, but not intrusive, and is undertaken:

a) for the purposes of a specific investigation or a specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

Intrusion

2.3 Surveillance becomes intrusive if the covert surveillance is:

a) carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or

c) carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

2.4 Before any officer of the Council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within the 2000 Act. In order to do this the following key questions need to be asked.

When Is Surveillance Covert?

2.5 Surveillance is covert when it is carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place.

2.6 If activities are open and not hidden from the subjects of an investigation, it is not covert and the 2000 Act framework does not apply. For example, Council House CCTV cameras in or outside the building which are readily visible to anyone walking around the building covered are overt in nature and so outside of the 2000 Act framework. If their usage is to monitor general activities e.g. what is happening in the car park, within the reception area, etc. their use and operation is outside of the scope of the 2000 Act even if, used in that way, they capture information that is of some evidential merit.

Specific Investigation or a Specific Operation?

2.7 If the CCTV cameras are targeting a particular known individual, and are being used to monitor his or her activities, the investigation has turned into a specific operation which will require authorisation.

Does It Involve Obtaining Private Information About A Person?

2.8 **Private information** is any information relating to a person's private or family life, including professional or business relationships. Forexample, if part of an investigation is to observe a member of staff's home to determine their comings and goings, then while that might be a legitimate purpose to undertake surveillance, the principles of necessity, proportionality and collateral intrusion will need to be considered to ensure that the need for the surveillance remains justifiable and proportionate to the end result that the investigation sets out to achieve.

2.9 If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework.

If in doubt, it is safer to get authorisation.

An Immediate Response to Events or Circumstances?

2.10 The Home Office gives the example of anything happening as an immediate response to something happening during the course of an observer's work, **and** which is unforeseeable.

2.11 However if as a result of an immediate response, a specific investigation subsequently takes place, the ensuing investigation brings it within the 2000 Act framework.

Is The Surveillance Intrusive?

2.12 Directed surveillance turns into intrusive surveillance if carrying it out involves anything that occurs on residential premises or in any private vehicle, and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device – see paragraph 2.3 earlier.

2.13 If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

As previously noted in paragraph 1.9, the Council is not authorised to

carry out intrusive surveillance.

Authorisations

2.14 The statutory requirement is that authorisations may only be issued by a Director, Head of Service or Service Manager. Note however that here at Derby, the constitution restricts the exercise of the power to 'Director' only. However, directed surveillance likely to result in obtaining confidential information, or involving the use of juveniles or vulnerable persons as informants, may only be authorised by the 'Head of the Paid Service' i.e. the Chief Executive, or his or her deputy in their absence.

2.15 For directed surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes that:

a) the 'threshold test' has been met i.e. it involves the investigation of the commission of an offence which, if proven, carries a minimum 6-month sentence of imprisonment;

b) that an authorisation is necessary for the purpose of **preventing or detecting crimeor of preventing disorder**; and

c) that the need for surveillance is proportionate to what is sought to be achieved by carrying it out.

NB: In relation to the 'threshold test' at (a) that there is one exception to the test. It is that the threshold test does not apply to investigations involving surveillance of offences involving the sale of alcohol or tobacco to under-aged persons. This exception will be of specific relevance to Trading Standards and Licensing enforcement personnel.

2.16 The onus is therefore on the person authorising the surveillance to satisfy themselves it is:

a) necessary on the above ground; and

b) proportionate to its aim.

In considering the question or proportionality, authorising officers should ask themselves whether the evidence can be obtained in any other way without the need for the formal grant of an authorisation. The Home Office Code of Practice says on this point:

"…if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet objective in question and must not be arbitrary or unfair".

2.17 In order to ensure that authorising officers have sufficient information in order to make an informed decision, it is important that detailed records are maintained. As such, the forms in Appendix 2 are to be completed where relevant. Subject to appropriate justifications being in place, it would also be prudent to make any authorisation sufficiently wide enough to cover all the surveillance methods to be deployed, as well as being able to demonstrate effective monitoring of what has been done against what was authorised.

2.18 It is important that the officer undertaking the operation/investigation immediately notifies the authorising officer if, in the course of undertaking those duties, there is unexpected interference with the privacy of individuals who are not the original subject of the operation/investigation, or who are not covered by the authorisation in some other way.

2.19 It is possible that in these circumstances, the original authorisation may not be sufficient for the continued purpose of the investigation and consideration should be given to whether a new or separate authorisation is required. The authorising officer faced with such a request should, as with every other authorisation, re-assess the

merit of the request on grounds of necessity and proportionality, and in particular consider whether or not the evidence could be obtained in another way without the need for continued surveillance.

Requirements of the 2000 Act

2.20 Unless the circumstances are demonstrably urgent, all authorisations must be in writing. In Appendix 2 to this guidance are links to the standard forms which must be used. Officers must direct their minds to the circumstances of the individual case with which they are dealing when completing the form. For urgent grants or renewal, oral authorisations are acceptable.

2.21 All authorisations for directed surveillance must be cancelled once the purpose for which the authorisation was sought/obtained have been achieved, even if that occurs on a date earlier than the indicated terminal date (if any) stated on the application.

Authorisations expire, if not renewed, in all cases, 3 months from the date of grant or latest renewal.

2.22 An authorisation can be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms.

2.23 Investigators are reminded to have regard to the new oversight provisions contained in chapter 7, requiring draft applications to be forwarded to Legal Services prior to formal authorisation.

2.24 Since 1 November 2012, there is now a requirement for all authorisations issued by the Council to be approved by the magistrates‟ court, by the grant of an Order. Magistrates‟ approval is required for the grant or renewal of authorisations, before the authorisation becomes effective. There is no requirement for magisterial approval of reviews or cancellations but the absence of (a) review(s) is likely to be challenged by the magistrates‟ if a renewal is being sought from them.

2.25 The magistrates need to be satisfied that:

(1) the statutory tests have been met (i.e. threshold, rank and that the rank officer is properly authorised); and
(2) that the code tests have also been met i.e. the use of surveillance is both necessary and proportionate.

2.26 At the conclusion of the hearing into the merit of the application, the magistrates may decide either to:

(a) approve the authorisation;
(b) refuse the authorisation; or
(c) refuse and quash the authorisation.

The difference between (b) and (c) is that with the former, there is scope for the Council to go back and refine the application to overcome any shortcomings identified by the magistrates.

2.27 The magisterial approvals process envisages that those who appear before the magistrates to make the application for an Order are specifically authorised / delegated by the Council to do so. This means that Council officers requesting approval can expect the magistrates to ask to see proof of delegation to such officers, entitling them to request the Order. It also envisages that those appearing before the magistrates have an operational awareness of the background to the matter, to assist with informing the magistrates about the necessity and proportionality merits of the applications.

Magistrates" may also query the authorising officers" (i.e. Director's) justifications for authorising the application. Consequently, both authorising officers (Directors) and case officers should be prepared to attend at court when following an authorisation being issued, when approval is sought.

Factors to Consider

2.28 Any person giving an authorisation should first satisfy him/herself that the authorisation is necessary on particular grounds and that the surveillance is proportionate to what it seeks to achieve.

2.29 The principle of **necessity** requires that applicants must ensure that they specify the particulars of the offence under investigation, ideally by reference to the applicable legislative provision that has been breached. A short explanation of the offence, the details of the perpetrator, the victim or witness and the telephone or internet address, and how each of these link in with the application being made should be detailed. The source of the telephone number or internet address should also be outlined. An Authorising Officer will seek reasoning that the conduct is necessary for the statutory purpose, ie 'the prevention or detection of crime or the prevention of disorder'. The Authorising Officer must be satisfied that there is an identifiable offence to detect or prevent before authorisation is given.

2.30 The principle of **proportionality** must consider three essential elements:

(a) that the proposed covert surveillance is proportional to the mischief under investigation
(b) that it is proportional to the degree of anticipated intrusion on the target and others; and
(c) it is the only option, other overt means having been considered and discounted.

and requires an explanation from the applicant about their specific justifications for considering surveillance, or the use of a CHIS, is appropriate in the circumstances of the application they are making. Doing so should enable applicants to demonstrate how the level of intrusion is considered to be justified when taking account of the benefit to be derived from acquiring the information.

2.31 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons other than the subject(s) of the surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example premises used by lawyers, any form of medical or professional counselling or therapy or in churches, mosques, synagogues or other place of faith worship.

2.32 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises would not be considered as intrusive surveillance.

2.33 The principle of **collateral intrusion** requires the applicant to demonstrate that s/he has considered the likelihood that through the process of acquiring the information sought, they are aware of the possibility that they might obtain information that is outside the realms of the investigations in question and then outline how, if that occurs, they plan to manage that process and/or the information so obtained.

2.34 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. This must be taken into account by the authorising officer, particularly when considering the proportionality of the surveillance.

2.35 Those carrying out the covert surveillance should inform the authorising officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation, or are covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a new separate authorisation is then required.

2.36 Any person giving an authorisation will also need to be aware of particular sensitivities inthe local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

Home Surveillance

2.37 The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his/her home, or where there are special sensitivities.

Any person undertaking such surveillance must be alert to the need to avoid intrusion of the subjects or other third parties privacy, remembering always that authorisations granted by the Council cannot, and do not, authorise intrusive surveillance.

Spiritual Counselling

2.38 No operations will be undertaken in circumstances where investigators believe that surveillance will lead to them intrude on spiritual counselling between a Minister and a member of his/her faith. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity where the person being counselled is seeking, or the Minister is imparting, forgiveness or absolution of conscience.

Confidential Information

2.39 The 2000 Act does not provide any special protection for `confidential material'. Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. Such material is particularly sensitive, and is subject to additional safeguards under the Code of Conduct. In cases where the likely consequence of the conduct of surveillance is likely to involve a person acquiring knowledge of a target's confidential information, the directed surveillance should be authorised by a Strategic Director or, in the case of the deployment of the source likely to access such information, special authorisation by the Chief Executive.

2.40 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

2.41 The following general principles apply to confidential material acquired under Part II authorisations:

- Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Legal Division before further dissemination takes place.

- Confidential material should not be retained or copied unless it is necessary for a specified purpose.

- Confidential material should only be acquired and/or disseminated where an appropriate officer i.e. a Director or the Chief Executive (having sought advice from a legal adviser) is satisfied that doing so is both necessary and proportionate for a specific purpose.

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

Handling and Disclosure

2.42 Authorising Officers are reminded of the guidance relating to the retention and

destruction of confidential material.

2.43 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

2.44 Authorising Officers must ensure that ALL ORIGINAL RIPA applications / authorisations, reviews, renewals and cancellations should be sent to the RIPA Co-ordinating Officer for inclusion in the Central Record. The RIPA Co-ordinating Officer is detailed at Appendix 3.

2.45 Applications for directed surveillance are to be retained by the Authorised Officer, for a period of 5 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

2.46 Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation nor to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

2.47 There is nothing in the 2000 Act that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the authority that authorised the surveillance, of any material obtained by means of covert surveillance, and other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

3 COVERT USE OF HUMAN INTELLIGENCE SOURCES (CHIS)

Background

3.1 There are occasions when the Council may use an external or professional source for the purpose of obtaining information. Also, it is potentially possible that the role of a Council employee may be that of a source in the course of an investigation. These situations are expected to arise very rarely, if at all.

3.2 Nothing in the 2000 Act prevents material obtained by an external or professional source, or an employee acting as a source, from being used as evidence in Court proceedings.

3.3 The Act makes provisions for the use and management of the so-called "Covert Human Intelligence Source" (CHIS). Under section 26(8) of the 2000 Act a person is a CHIS if:

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

3.4 In every such case, the Authorising Officer must consider the safety and welfare of the source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before an authorisation is given. Consideration must be had from the start for the safety and welfare of the source, even after cancellation of the authorisation.

3.5 The 2000 Act places duties on the Council for the effective management (and welfare) of a CHIS, as follows:

Tasking

Is the assignment given to the source by their controller, asking the source to obtain information, provide access to information or otherwise act in a defined way. The source's designated contact (normally the investigating officer or team leader) will have day to day responsibility for:

- dealing with the source on behalf of the Council
- directing day to day activities of the source
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

Authorisations may cover a range of activities under which the source may be tasked. If however, it is intended to task the source in a new or significantly greater way than originally authorised, the authorising officer should be informed and consideration given to completing a separate authorisation form.

Management Responsibility

Clear management arrangements must be in place for all sources. The source will have a designated person for day to day contact normally the Investigating Officer or Team Leader. It will be the responsibility of each department to record any form contact held with the source during the course of the authorised activity.

Security and Welfare

The Council must take account of the welfare of the source in authorising or tasking of a source. Before authorisation, the Authorising Officer should ensure that a Risk Assessment form has been completed to determine risk to the source of any tasking and the likely consequences should the role of the source become known. Ongoing security and welfare, post cancellation of the authorisation should also be monitored.

The Investigating Officer is responsible for informing the Authorising Officer of any concerns which might affect:

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

3.6 The Authorising Officer must believe that the authorised use of the source is proportionate to what it seeks to achieve. Accurate and proper records should be kept about the source and the tasks undertaken.

3.7 Before authorising the use of a source, the authorising officer should have a reasonable belief that the conduct/use of the source in that manner, including the likely degree of intrusion into the privacy of those potentially affected, is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subject(s) of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

3.8 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, confidential material is likely to be obtained.

3.9 A person is a Covert Human Intelligence Source if:

a) s/he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph b) or c);

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

c) s/he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

3.10 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.

3.11 The above covers the use of professional witnesses to obtain information and evidence. A professional witness is a person who has knowledge of, has received training in or is certified to undertake certain actions of such a nature that are relevant to the to the specific discipline to which an investigation or operation is targeted, with the aim of collating evidence to assist the process of that investigation or operation e.g. a professional witness may occupy an empty Council house in order to obtain evidence of anti-social behaviour in relation to a next door neighbour in circumstances where other neighbouring residents decline to assist that process for fear of reprisal from the perpetrator. This role is to be contrasted to that of an 'agent provocateur', which is dealt with below.

3.12 Inducement of a target to commit an offence of then nature under investigation, whether by the CHIS or other avenue, by means of oppression, duress or wheedling (which require an officer to 'encourage' the act constituting the offence to take place (i.e. acting as an agent provocateur)) is not permitted regardless of the provisions of the 2000 Act.

3.13 It should be remembered that if a CHIS is to be safely deployed, there would be a need to have in place for the proper and effective management of the source, trained handlers and controllers each of whom would need to be trained. The reality is that it would be extremely unusual for the Council to need to employ the use of a CHIS within an investigation or operation. There is a need to strike the right balance between the cost involved in securing that training when weighed against the unlikeliness that a CHIS authorisation will be granted. Officers considering deploying a CHIS should first seek advice from the Director of Legal & Democratic Services as a matter of urgency.

3.14 The use of a CHIS, like directed surveillance, is based on the principles of Article 8 of the European Convention on Human Rights.

If in doubt it is safer to obtain authorisation.

Authorisations

3.15 As with directed surveillance, the same broad principles relating to necessity, proportionality and collateral intrusion are equally applicable to CHIS authorisations. In the interest of brevity, they are therefore not repeated separately here but investigators considering deploying a CHIS are referred to that earlier text at paragraphs 2.28 – 2.30, and 2.32 and 2.33 (above). Similarly, the statutory requirement that authorisations may only be issued by a Director, Head of Service or Service Manager applies to CHIS', noting the local Derby constitutional restriction to 'Director' only. It is also worth reiterating that directed surveillance likely to result in obtaining confidential information, or involving the use of juveniles or vulnerable persons as informants, may only be authorised by the 'Head of the Paid Service' i.e. the Chief Executive, or his or her deputy in their absence.

Any of the Authorising Officers listed in Appendix 3 can authorise a CHIS.

3.15a Please note that ONLY the Chief Executive or in his / her absence, whoever deputises for him / her, may authorise the employment of juvenile or vulnerable CHIS or the acquisition of confidential information.

Please note that the duration of an authorisation for a juvenile CHIS is one month.

3.16 The conduct to be authorised is any conduct that:

a) involves the investigation of the commission of an offence which, if proven, carries a minimum 6-month sentence of imprisonment; OR

b) the offence is an offence under

i) Sections 146, 147 or 147A of the Licensing Act 2003; OR
ii) Section 7 of the Children and Young Persons Act 1933.

c) is comprised in any such activities involving conduct of a covert human intelligence source, or the use of a covert human intelligence source, as are specified or described in the authorisation;

d) consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and

e) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

3.17 In order to ensure that authorising officers have sufficient information in order to make an informed decision about whether or not to issue an authorisation, it is important that detailed records are maintained. As such the forms attached in Appendix 2 are to be completed where applicable.

3.18 It would also be prudent to make any authorisation sufficiently wide enough to cover all the surveillance means required for a specific investigation, as well as being able to prove effective monitoring of what has been done against what was authorised.

Requirements of the 2000 Act

3.19 Unless the circumstances are demonstrably urgent, all authorisations must be in writing. In Appendix 2 to this guidance are links to standard forms which must be used. Officersmust direct their minds to the circumstances of the individual case with which they are dealing when completing the form.

3.20 All authorisations for the use of a CHIS must be cancelled once the purpose for which the authorisation was sought/obtained have been achieved, even if that occurs on a date earlier than the indicated terminal date (if any) stated on the application. CHIS authorisations otherwise expire, if not renewed, 12 months from the date of last renewal.

3.21 An authorisation can be renewed at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms.

3.22 Authorising officers should not renew a CHIS authorisation unless a review has been carried out and that person has considered the results of the review when deciding whether to renew or not. A review must consider what use has been made of the source, the tasks given to them and the nature and quality of the information obtained.

3.23 Investigators are reminded to have regard to the new oversight provisions contained in chapter 7, requiring draft applications to be forwarded to Legal Services prior to formal authorisation.

Applications

3.24 As with Directed Surveillance activity, since 1 November 2012, there is now a requirement for all CHIS authorisations issued by the Council to be approved by the magistrates‟ court, by the grant of an Order. To that end, the detail contained in paragraphs 2.23 – 2.26 of this guidance is equally applicable in relation to CHIS applications, as it is to Directed Surveillance, and should be read as such.

Management of Covert Human Intelligence Source

3.25 When using a CHIS arrangements must be in place to ensure proper oversight and management of CHIS, including the appointment of individual officers defined as 'Handlers' and 'Controllers' (defined by Sections 29(5) (a) and (b) RIPA 2000) for each CHIS.

Role of a Handler

3.26 The Handler will usually hold a position in the Council below that of the Authorising Officer.

The Handler will have day-to-day responsibility for:

- dealing with the CHIS on behalf of the Council
- directing the day-to-day activities of the CHIS
- recording the information supplied by the CHIS
- monitoring the CHIS' welfare and security.

The Controller

3.27 The Controller will normally be responsible for the management and supervision of the 'Handler' and general oversight of the use of the CHIS.

Security and Welfare of the CHIS

3.28 Prior to authorisation, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known.

The ongoing security and welfare of the CHIS should also be considered following the cancellation of the authorisation.

The CHIS Handler is responsible for bringing to the Controller's attention any concerns about personal circumstances of the CHIS insofar as they may affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

Where appropriate, concerns must be considered by the Authorising Officer and a decision taken on whether or not to allow the Authorisation to continue.

4 COMMUNICATIONS DATA

4.1 Communications data is information held by Communication Service Providers (CSP) (e.g. telecom, internet and postal companies) relating to the communications made by their customers. The 2000 Act makes provision for obtaining communications data from such service providers and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself (i.e. traffic data - contents of e-mails).

4.2 Examples of “data” available to the Council under the Act include:

- Postal items - anything written on the outside of the envelope
- Telephone subscriber information - personal details of the subscriber, the telephone number and itemised calls made.
- E-mail & Internet subscriber information – details of the subscriber of email account, websites visited, details of the date and time emails sent and received.

4.3 Similarly to the procedures relating to both directed surveillance and CHIS, communications data can only be obtained for the sole category of **for the prevention and detection ofcrime and/or disorder**. There is also the requirement to ensure that the test of **necessity** is met before data is obtained. It is the responsibility of the Authorising Officer to undertake that test. In addition, the Authorising Officer must also consider that the conduct involved in obtaining the communications data is **proportionate** to the aim that it is sought to achieve. In carrying out these assessments, the Authorising Officer must remain alert to the risk of collateral intrusion which is to be avoided unless such intrusion can be justified.

4.4 The principle of **necessity** requires that applicants must ensure that they specify the particulars of the offence under investigation, ideally by reference to the applicable legislative provision that has been breached. A short explanation of the offence, the details of the perpetrator, the victim or witness and the telephone or internet address, and how each of these link in with the

application being made should be detailed. The source of the telephone number or internet address should also be outlined.

4.5 The principle of **proportionality** requires an explanation from the applicant about why specific date or time periods of data are being sought, and what the applicant expects to achieve from obtaining the data. Doing so should enable applicants to demonstrate how the level of intrusion is considered to be justified when taking account of the benefit to be derived from acquiring the data. It may be prudent at this stage to outline what other less intrusive forms of investigation have been considered or tried, and why the applicant deems such measures either to not be feasible or to have failed.

4.6 The principle of **collateral intrusion** requires the applicant to demonstrate that s/he has considered the likelihood that through the process of acquiring the data, they are aware of the possibility that they might obtain information that is outside the realms of the investigations in question and then outline how, if that occurs, they plan to manage that process and/or the information so obtained.

Applying for Communications Data

4.7 There are two independent routes by which the Act allows communications data to be obtained from service providers. These are either:

(i) the granting of **Authorisations;** or
(ii) the service of **Notices.**

Authorisation

4.8 An Authorisation allows the Council to collect or retrieve data itself from the CSP. An authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the Communications Data;
- it is believed that 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 Council and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

Notice

4.9 This is the more likely method by which communications data will be retrieved by the Council. A Notice is given by the Council to a postal or telecommunications operator that requires the operator to collect the data and provide it to the Council.

Roles

4.10 Within the Council, there are four distinct roles involved in the process of accessing / obtaining communications data, namely:

(i) The **applicant** is the person involved in conducting an investigation or operation. Within the Council, this would normally be the case officer. The applicant begins the process by completing an application form, setting out within the form for consideration by the Authorising Officer sufficient detail justifying the need for the data in question to be accessed;

(ii) The applicant then forwards the application to the Council's **Single Point of Contact(SPoC)**. The SPoC is an accredited individual (and hence is sometimes referred toas an Accredited Officer) trained in the process of facilitating the lawful acquisition of communications data and acts as the go-between between the Council and the CSP;

(iii) The SPoC will forward the application to the **Authorising Officer**. It is the role of the Authorising Officer to satisfy him or her self about the necessity and proportionality of the application, and that there either is no collateral intrusion involved in the investigation or that any such intrusion is justifiable. They will make that assessment strictly on the basis of the information contained in the application. If so satisfied, they sign off the application and return it to the SPoC, who then

sends it to the CSP;

(iv) The **Senior Responsible Officer** is responsible for ensuring the integrity of the process in place within the Council for acquiring communications data. The post holder is responsible for ensuring compliance with the communications data provisions of the 2000 Act, the oversight responsibility for identifying errors, ensuring that adequate processes are in place to minimise repetition of errors and reporting of errors to the Commissioner.

4.11 Details of the posts within the Council that undertake each of these roles are contained in Appendix 3. In relation to the Authorising Officer role, it is anticipated that the vast majority of authorisations will be granted /issued by the Director of Environment and Regulatory Services, with the Head of Legal Services (General) occupying his post as a reserve.

The Application Process

4.12 An application for accessing communications data needs to be completed together with the Notice. As with the other methods of surveillance, these forms have been standardised by the Council and are available within the document library on DerbyNet. The applicant will need the following information to complete these forms:

- a unique reference number (URN)
- the operation and person (if known) to which the requested data relates;
- a description, in as much detail as possible, of the Communications Data requested;
- the reason why obtaining the requested data is considered to be necessary;
- an explanation of why obtaining the data constitutes conduct proportionate to what it seeks to achieve;
- a consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified;
- the timescale within which the Communications Data is required. Where the timescale within which the material is required is any greater than routine, the reasoning for this is to be included.

4.13 An authorised application form should subsequently record whether access to communications data was approved or denied, by whom and the date. Alternatively, the application form can be marked with a cross-reference to the relevant notice. Both the application and the Notice form then need to be checked by the SPoC.

4.14 The SPoC's role, while primarily a conduit for the transmission of information between the Council and the CSP, also promotes good practice by ensuring that only practical and lawful communications data requests are made. The SPoC provides objective judgement and advice to both the applicant and the Authorising Officer.

The SPoC will complete a log sheet that records details of each application they have considered, the dates they were received, who from, when forwarded to the Authorising Officer, the date when the Notice (or Authorisation) is returned to the SPoC, when the SPoC forwarded on the Notice to the CSP, when results were received from the CSP and summaries of all communications exchanged between the SPoC and the CSP during the processing of the Notice (or Authorisation).

4.15 The Council has two accredited SPoCs, whose details appear in Appendix 4. It is a requirement that a person carrying out the functions of a SPoC must have successfully completed the relevant SPOC training for the purposes of dealing with communications data. SPoCs should be in a position to:

- assess whether access to communications data is reasonably practical for the postal, internet or telecommunications operator;
- advise applicants and Authorising Officers on the practicalities of accessing different types of communications data from different postal, internet or telecommunications operators;
- advise applicants and Authorising Officers 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 Council and

the postal, internet or telecommunications operator.

Once the SPoC has satisfied himself of these issues, they then forward the application and notice onto the Authorising Officer.

4.16 The Authorising Officer's role is as set out in paragraph 1.3 – to be satisfied that the dual tests of necessity and proportionality are met and that there is no collateral intrusion, or else that any such intrusion can be objectively justified. Where the application is based on grounds of urgency, he or she must also be satisfied that any such grounds are justified.

The Authorising Officer will base his or her decision solely on the content of the application form, which is never sent to the CSP. If so satisfied, then they grant an Authorisation or give a Notice. The Authorisation or Notice is then returned to the SPoC for the SPoC to send out to the CSP.

4.17 An Authorising Officer must not grant an Authorisation or give a Notice on a matter in which they are directly involved.

4.18 The Notice served on the CSP must contain the following information:

- a description of the required communications data;
- for which of the purposes the data is required;
- the name, office, rank or position of the Authorising Officer; and
- the manner in which the data should be disclosed.

4.19 The Notice should also contain:

- a Unique Reference Number (URN) obtained from the relevant CSP;
- where appropriate, any indication of any urgency;
- a statement stating that data is sought under the provisions of Chapter II of Part 1 of the 2000 Act, ie an explanation that compliance with the Notice is a legal requirement; and
- contact details so that the veracity of the Notice may be checked.

4.20 Authorising Officers should be of the same level of seniority as identified within the forms of directed surveillance and CHIS dealt with earlier in this policy document.

Urgent Requests

4.21 An application for communications data may only be made and approved orally, on an urgent basis, where it is necessary to obtain the data in an emergency i.e. where life would be endangered or the investigation jeopardised. Urgent oral authorisations have a duration of 72 hours commencing from the time when the authorisation was granted.

Duration of Authorisations and Notices

4.22 Authorisations and Notices are only valid for **one month**. This period will begin when the Authorisation is granted or the Notice given. The Authorising Officer should specify a shorter period if s/he is satisfied by reference to the detail contained in the request of the appropriateness of doing so, since this may go to the proportionality requirements. For 'future' applications, communications data disclosure may only be required of data obtained by the postal, internet or telecommunications operator **within** a period of up to one month.

For 'historical' applications, communications data disclosure may only be required if it is in the possession of the postal, internet or telecommunications operator. A postal, internet or telecommunications operator should comply with a Notice as soon as is reasonably practicable.

4.23 Reviews should be undertaken during the authorised period to assess the continuing need for/use of communications data. The frequency of review will be determined by the Authorising Officer in the context of the investigation and taking particular account of access to confidential

information and collateral intrusion. Records of review should be forwarded to the SPoC for inclusion in the central record.

Renewal

4.24 An Authorisation or Notice may be renewed at any time during the month it is valid, by following the same procedure as in obtaining a fresh Authorisation or Notice. A renewed Authorisation or Notice takes effect at the point at which the Authorisation or Notice it is renewing expires.

4.25 Authorisation of renewals will normally be made by the original Authorising Officer unless it is not reasonably practicable to do so, in which event the reserve Authorising Officer may authorise renewal. Authorisations may be renewed more than once provided they continue to meet the criteria for Authorisation.

4.26 Application for renewals must include the following information:

- whether this is the first renewal or details of every occasion on which the authorisation has been renewed previously;
- any significant changes to the information supplied in the original application;
- reasons why it is necessary to continue the surveillance;
- content and value to the investigation/operation of the information already obtained;
- result of reviews of the investigation.

Cancellation

4.27 The Authorising Officer should cancel a Notice as soon as it is no longer **necessary,** or the conduct is no longer **proportionate** to what is sought to be achieved. The duty to cancel a Notice primarily falls on the Authorising Officer who issued it.

4.28 In relation to the service of a Notice, the relevant CSP will need to be informed of the cancellation.

4.29 Records of cancellations are recorded on a separate form. An Authorising Officer who cancels a Notice should ensure that they forward notification of the cancellation to the SPoC for recording/retention within the central register.

Guidance

4.30 More detailed guidance for applicants on the principles of necessity, proportionality and collateral intrusion is provided in a separate guidance note 'Guidance to Applicants for Communications Data' which can be found on DerbyNet.

Training

4.31 The Council is committed to ensuring that all of its employees, at whatever level, involved in the administration, processing and acquisition of communications data are properly trained for that purpose. The need for refresher training will be considered at least annually. All employees involved in the communications data process are encouraged to raise any emerging training needs with either of the Council's SPoC's, Authorising Officers or the Senior Responsible Officer.

5 CODES OF PRACTICE

5.1 There are Home Office Codes of Practice that expand on this guidance. Copies are held by the Director of Legal & Democratic Services for access by the public.

5.2 The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, *"if any provision of the code appears relevantto a question before any Court or tribunal considering any such proceedings, or to the tribunal established under the 2000 Act, or to one of the commissioners responsible for overseeing the powers conferred by the 2000 Act, it must be taken into account"*.

5.3 Staff should refer to the Home Office Codes of Conduct for supplementary guidance. There are separate codes for directed surveillance, use of a CHIS and for communications data. Copies are also available for consultation on the Council's intranet (DerbyNet) which can be accessed by typing in 'RIPA' as the relevant search criteria.

6 CENTRAL REGISTER OF AUTHORISATIONS

6.1 The 2000 Act requires a central register of all authorisations to be maintained. There are two such registers in operation, one in relation to Directed Surveillance and CHIS operations, and the second in relation to Communications Data. The Council's Director of Legal & Democratic Services maintains both these registers.

6.2 Whenever an authorisation is granted, whether for directed surveillance or CHIS, the Authorising Officer must arrange for the original authorisation to be forwarded to the Director of Legal & Democratic Services within 7 days of issue. The same principle applies in relation to cancellation, renewal and review forms. The Authorising Officer is advised to ensure that a copy of any issued form is maintained on the case/operation file. For communications data authorisations, the SPoC maintains a central register of all applications made, and Authorisations or Notices refused or granted.

6.3 It is each department's responsibility to securely retain copies of all authorisations within their departments. An authorisation should only be held for as long as it is necessary. Once an investigation is concluded (bearing in mind cases may be lodged some time after the initial work began) the records held by the department should be disposed of in an appropriate and secure manner (e.g. shredding).

7 OVERSIGHT

Senior Responsible Officer:
Janie Berry
Director of Legal and Democratic Services
Tel: 01332 643616
Email: janie.berry@derby.gov.uk

Responsibilities of the SRO

Within every relevant public authority a senior responsible officer must be responsible for:

- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with this code;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the OSC inspectors when they conduct their inspections, where applicable, and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

Within local authorities, the senior responsible officer should be a member of the corporate leadership team and should be responsible for ensuring that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed.

RIPA Co-ordinating Officer

Olu Idowu
Head of Legal Services
Tel: 01332 643615

Email: olu.idowu@derby.gov.uk

Responsibilities of the RIPA Co-ordinating Officer

The Co-ordinating Officer has day-to-day responsibilities for:

- maintaining the Central Record of Authorisations and collating the original authorisations / applications, reviews, renewals and cancellations
- oversight of submitted RIPA documentation
- organising a RIPA training programme
- raising RIPA awareness within the Council.

8 TRIBUNAL & SCRUTINY

8.1 To effectively "police" the 2000 Act, Commissioners regulate the conduct of the powers exercised by virtue of its provisions. The Chief Surveillance Commissioner will keep under review, among others, the exercise and performance by the persons on whom are conferred or imposed, the powers and duties under the Act. This includes authorising directed surveillance and the use of covert human intelligence sources.

8.2 A tribunal has been established to consider and determine complaints made under the 2000 Act. Complaints can be made to the tribunal by persons aggrieved by conduct exercised by virtue of the 2000 Act e.g. directed surveillance. The forum hears applications on a judicial review basis. Claims should ordinarily be brought within one year unless it is just and equitable to extend that.

8.3 The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person. Local authorities are, however, under a duty to disclose or provide to the tribunal all documents the tribunal requires if:

- the authority has granted any authorisations under Part II of the 2000 Act;
- the authority has engaged in any conduct as a result of the authorisation;
- an individual employed by it holds a rank, office and position within the authority for whose benefit any such authorisation has been or may be given;
- a disclosure notice requirement is given.

8.4 In accordance with the Act, the Council's Audit and Accounts Committee will be provided with updates on the implementation and administration of the Council's RIPA functions.

APPENDIX 1

DEFINITIONS FROM THE 2000 ACT

"1997 Act"	means the Police Act 1997
"2000 Act"	means the Regulation of Investigatory Powers Act 2000
"Confidential Material"	has the same meaning as it is given in Sections 98 -100 of the 1997 Act. It consists of: a) matters subject to legal privilege b) confidential personal information; or c) confidential journalistic material.
"Matters Subject To Legal Privilege"	Includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A below).
"Confidential Personal Information"	Is information held in confidence concerning anindividual (whether living or dead) who can be identified from it, and relating:

a) to his/her physical mental health; or

b) to spiritual counselling or other assistance given or to be given, and which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid of unpaid office(see Note B below). It includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

c) It is held subject to an express or implied undertaking to hold it in confidence; or

d) It is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

"Confidential Journalistic Material" Includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an

	undertaking.
"Covert Surveillance"	Means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

"Authorising Officer"	For the purposes of authorising directed surveillance under the 2000 Act, an "authorising officer" means the person designated for the purposes of Section 28 of the 2000 Act to grant authorisations for directed surveillance (see the Regulation of Investigatory Powers [Prescription of Offices, Ranks and Positions] Order) SI 2000 / 2417.
"Working Day"	Means any other day other than a Saturday, Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom.

Note A *Legally privileged communications will lose their protection if there is evidence, forexample, that the professional legal adviser is intending to hold or use them for acriminal purpose; privilege is not lost if a professional legal adviser is properlyadvising a person who is suspected of having committed a criminal offence. Theconcept of legal privilege shall apply to the provision of professional legal advice byany agency of organisation.*

Note B *Confidential personal information might, for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

Appendix 2

Standard Forms

These are available on DerbyNet by typing the following search criteria, 'RIPA', into the search field and clicking on 'Go'.

The following is a full list of the documents, together with hyperlinks to the form which can then be downloaded for use:

Directed Surveillance & CHIS

RIPA Form 1	-	Application for authorisation to carry out directed surveillance
RIPA Form 2	-	Cancellation of directed surveillance
RIPA Form 3	-	Application for renewal of directed surveillance authority
RIPA Form 4	-	Review of a directed surveillance authority
RIPA Form 5	-	Application for authorisation of the use or conduct of a covert human intelligence source (CHIS)
RIPA Form 6	-	Cancellation of an authorisation of the use or conduct of a covert human intelligence source (CHIS)
RIPA Form 7	-	Application for the renewal of an authorisation of the use or conduct of a covert human intelligence source (CHIS)
RIPA Form 8	-	Review of the use or conduct of a covert human intelligence source (CHIS)

Communications Data

RIPA Form 9	-	Application for Communications Data
RIPA Form 10	-	SPoC form for rejection of Communications Data application
RIPA Form 11	-	Communications Data Notice
RIPA Form 12	-	Cancellation Notice (Applicant or Authorised Officer to SPoC)
RIPA Form 13	-	None
RIPA Form 14	-	Authorised Officer's Considerationform
RIPA Form 15	-	Form for Reporting of Errors to the IOCCO

Other Documents

Code of Practice - Directed Surveillance

Code of Practice - CHIS

Code of Practice – Communications Data

APPENDIX 3

LIST OF OFFICERS

Directed Surveillance & CHIS Authorising Officers

Director of Customer Management

Director of Environment and Regulatory Services

Director of Younger Adults and Housing

Chief Executive (juvenile or vulnerable CHIS or acquisition of confidential information)

Senior Responsible Officer and RIPA Monitoring Officer

Director of Legal and Democratic Services

RIPA Co-ordinating Officer

Head of Legal Services

Communications Data Authorisations

Single Point of Contact:

(Head of Trading Standards and Bereavement Services)

Authorising Officer:

Director of Environment and Regulatory Services

APPENDIX 4

SUPPLEMENTARY GUIDANCE TO STAFF

1.1 The Human Rights Act 1998 (which became effective on 2 October 2000) incorporates into UK law the European Convention on Human Rights, the effect of which is to protect an individual's rights from unnecessary interference by the "State".

1.2 The relevant part of the Regulation of Investigatory Powers Act 2000 (RIPA), which came into force on 25 September 2000, regulates covert investigations by a "public bodies" and provides a framework within which the "State" (the specified public bodies) can work to ensure that law enforcement and other important functions can effectively protect society as a whole.

1.3 The Public Bodies defined in RIPA include Local Authorities and, therefore, Derby City Council's activities are subject to the *RIPA* framework.

1.4 The purpose of this guidance is to:

- explain the scope of RIPA and the circumstances where it applies
- provide guidance on the authorisation procedures to be followed.

1.5 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and these are available in the Legal Division, and can also be viewed or downloaded from the Home Office website by following the relevant link in Appendix 2.

1.6 There are a number of investigative techniques that are covered by RIPA. These are 'directed surveillance', 'intrusive surveillance' and the 'use of a covert human intelligence source' (CHIS). These are explained later in this document and the flowcharts that follow provide a straightforward approach to determining whether RIPA applies and, if so, which provisions apply.

1.7 The appropriate Service Director is responsible for authorising applications for directed surveillance or for the use of a CHIS in respect of the regulatory services for which they are responsible. In doing so, the Service Director must be satisfied that he or she is sufficiently removed from the investigation. It is accepted that they may deemed to manage it but they must not be involved in its day to day conduct (i.e.: they **MUST NOT take part** in the surveillance or in the management of the Covert Human Intelligence Source to which the application relates).

1.8 RIPA specifies that directed surveillance or the use of a CHIS can only be undertaken by a local authority for the following reason:

a) for the purpose of preventing or detecting crime or of preventing disorder;
~~b) In the interests of public safety;~~
~~c) for the purpose of protecting public health;~~
~~d) for the purpose of assessing or collecting any tax, duty, level or other imposition, contribution or charge payable to a government department;~~

~~e) for any other purpose specified by the Secretary of State;~~
~~f) For the protection of the rights and freedoms of others.~~

NB: The other statutory grounds are shown struck through, and are provided for information only.

1.9 Authorisation under RIPA gives lawful authority to carry out directed surveillance and to use a CHIS. Before approving applications, the Authorising Officer must have regard to the necessity, proportionality and subsidiarity elements of the application. Once authorised, an application must be made to the magistrates" court for an Order which permits the authorisation to be acted upon. Once the Order is obtained, the authorisation serves toprotect the Council and its officers from complaints of interference with the rights protected by Article 8 of the European Convention on Human Rights (the right to private and family life).

1.10 It should be noted that the Council does not, *under any circumstances,* have the power to undertake what is defined as 'Intrusive Surveillance'.

1.11 There are Home Office codes of practice that expand on the information in this guide and copies are available as indicated in paragraph 1.5, earlier.

The codes do not have the force of law, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, *"if any provision of the code appears relevant to aquestion before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account"*.

Staff should refer to the Home Office Codes of Conduct for supplementary guidance.

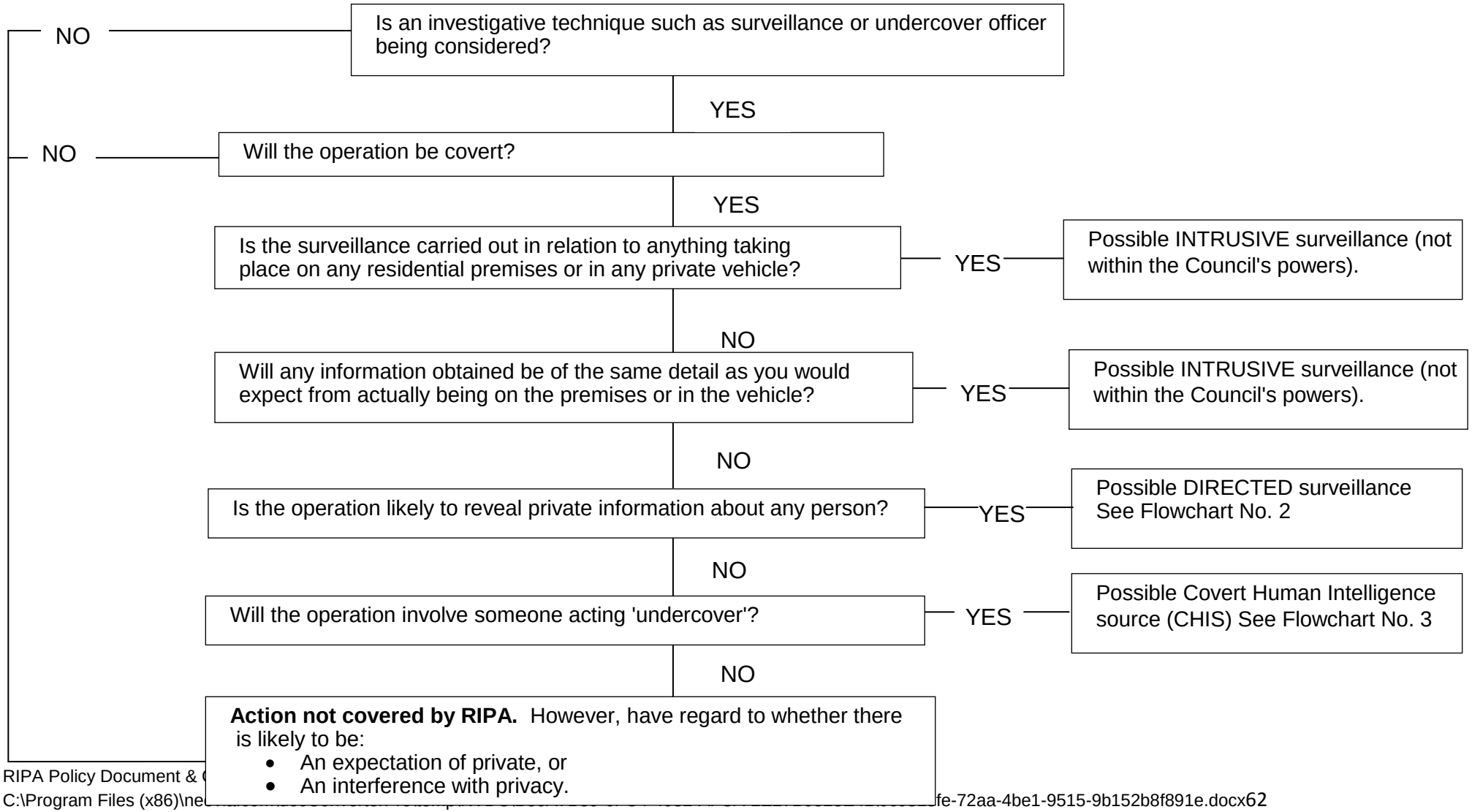
1.12 Deciding when authorisation is required involves making a judgement. If you are unclear about any aspect of the process, seek the advice of an Authorising Officer. If they are unable to answer your questions they must seek advice from the Council's Legal Services Division.

1.13 However, **IF YOU ARE IN ANY DOUBT** about whether a course of action requires an authorisation, **GET IT AUTHORISED.** (If you are unable to secure an authorisation it is likely that your application does not comply with the law).

1.14 Services within the Council that undertake surveillance that is covered by RIPA may wish to develop specific guidance on the applicability of RIPA to their particular circumstances. Such an approach is to be encouraged but the relevant Head of Service must ensure that any "local" guidance does not conflict with this corporate document.

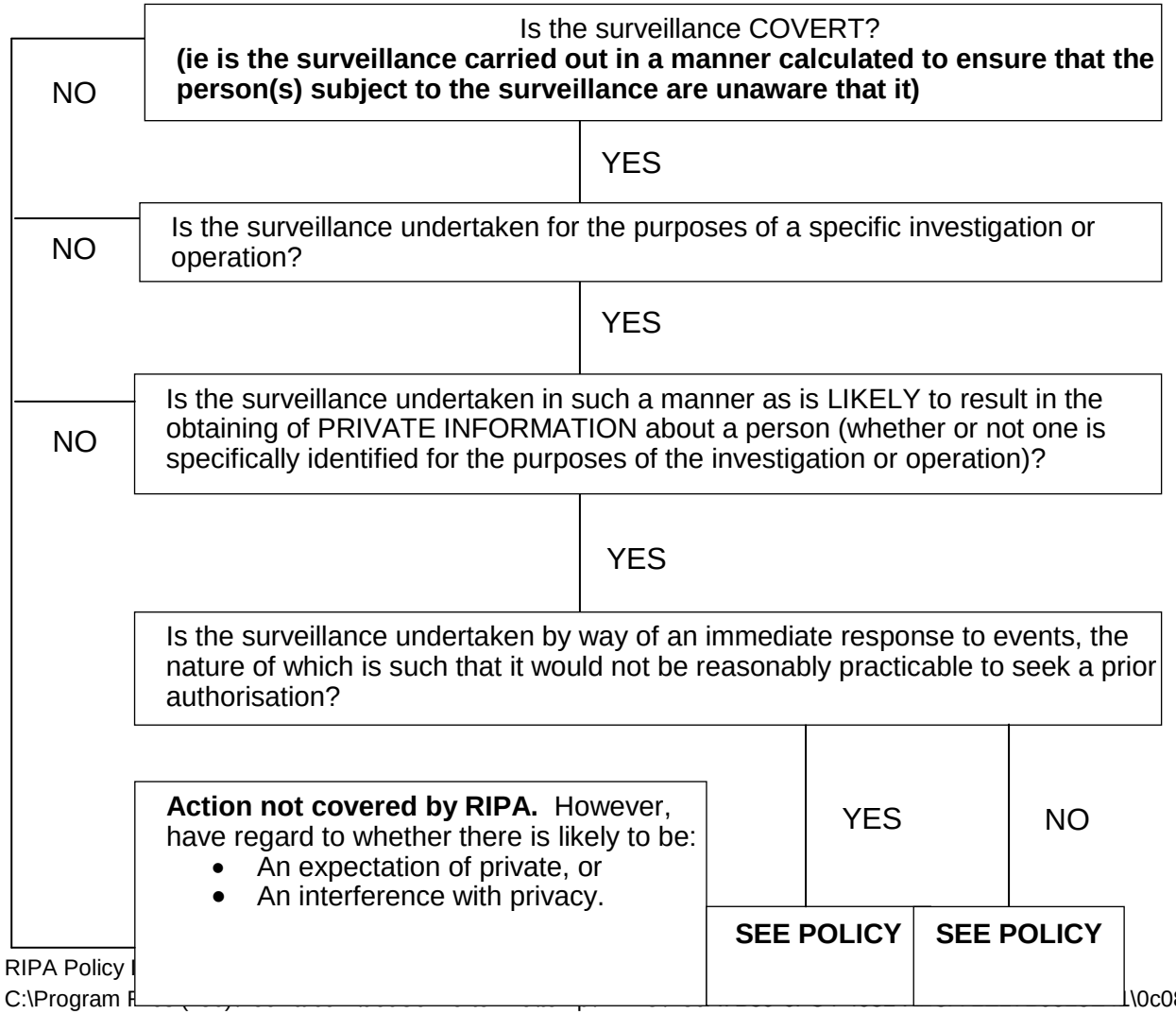
PROCESS FLOWCHARTS – No. 1

SURVEILLANCE SUMMARY



PROCESS FLOWCHARTS – No. 2

DIRECTED SURVEILLANCE



INTERPRETATION

COVERT see section 26(9) RIPA

SURVEILLANCE see Section 48)2) to 48(4) RIPA includes monitoring, observing or listening to persons, their movements, their conversations, or their activities or communications.

DIRECTED SURVEILLANCE see Section 26(2) RIPA.

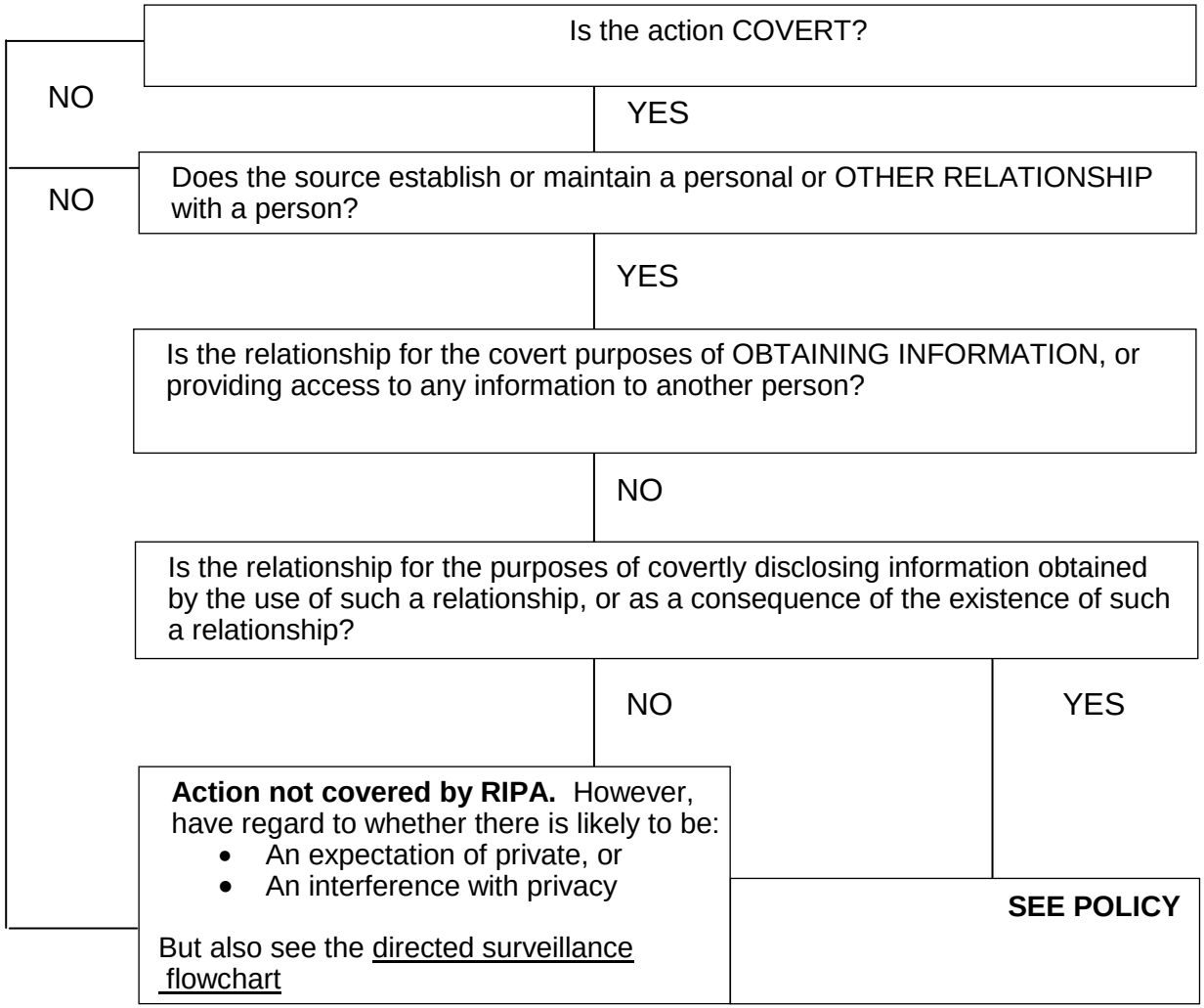
PERSON see Section 81(1) RIPA. Includes any organisation and any association or combination of persons.

PRIVATE INFORMATION see Section 26 (10) RIPA in relation to a person, includes any information relating to his private or family life. 'Private Information' should be given a wide interpretation and should not be restricted to what might be considered to be 'secret' or 'personal' information. Information that is in the open for all to see (for example, who is visiting a premise) may be deemed to be private information.

CONFIDENTIAL MATERIAL see paragraph 3 of the Code of Practice confidential information, includes matters subject to legal privilege, confidential journalistic material and confidential personal information, for example medical records or religious material.

For further interpretation see Sections 48 & 81 RIPA, including Explanatory Notes to RIPA & Codes of Practice on Covert Surveillance & Use of a CHIS.

COVERT HUMAN INTELLIGENCE SOURCE



INTERPRETATION

COVERT see section 26(9) RIPA

COVERT PURPOSES see Section 26(9)(b) & (c) RIPA.

CHIS see Section 26(8) RIPA. The use of a CHIS NOT surveillance (see Section 48(3) RIPA).

PERSONAL OR OTHER RELATIONSHIP This is not defined, but a wide interpretation should be applied.

INFORMATION This is not defined but section talks about information in general and is not restricted to private information as is the case with directed surveillance.

CONFIDENTIAL MATERIAL see paragraph 3 of the Code of Practice. Confidential information includes matters subject to legal privilege, confidential journalistic material and confidential personal information, for example medical records or religious material.

For further interpretation see Sections 48 & 81 RIPA, including Explanatory Notes to RIPA & Codes of Practice on Covert Surveillance & Use of a CHIS.