APPENDIX A

HARBOROUGH DISTRICT COUNCIL

POLICY AND GUIDANCE

DISTRICT OF HARBOROUGH
RURAL SOUTH LEICESTERSHIRE

FOR THE USE OF COVERT SURVEILLANCE, COVERT HUMAN INTELLIGENCE SOURCES ("CHIS") and THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

To comply with the Regulation of Investigatory Powers Act 2000 (as amended) and the Human Rights Act 1998 and having regard to the Codes of Practice published by the Secretary of State under S71 of the Regulation of Investigatory Powers Act 2000

CONTENTS

BACKGROUND

The Human Rights Act 1998 (which became effective on the 2nd 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".

The relevant parts of the Regulation of Investigatory Powers Act 2000 (*RIPA*) are Part II which came into force on 25th September 2000 and regulates covert investigations and Part 1 Chapter II, the acquisition and disclosure of communications data which came into force on 5th January 2004. These provide 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.

The Protection of Freedoms Act 2012 has amended RIPA to require that all authorisations made by an Authorising Officer of the Council must have Judicial Approval .

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

The purpose of this guidance is to:

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

The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and this is reproduced at Appendix 6. The supplementary guidance on the changes made by the Protection of Freedoms Act and its impact on the use of RIPA is reproduced at Appendix 7. They are also available on the *RIPA* section of the Policies part of the Council's Intranet. This can be found by accessing the Harborough District Council Intranet, double clicking on policies in the left hand column, clicking R on the alphabet selection or scrolling down to R to the Regulation of Investigatory Powers Act 2000 (RIPA). A guide to completing the RIPA forms for covert surveillance and CHIS can also be found within the same section.

1 RIPA - PART II COVERT SURVEILLANCE

INTRODUCTION

1.1 There are a number of investigation activities that are covered by *RIPA*. These are known as: Directed Surveillance; Intrusive Surveillance and the use of a Covert Human Intelligence Source (CHIS). These are explained later in this document and the flowcharts in Appendix 1 provide a straightforward approach to determining whether *RIPA* applies and, if so, which provisions apply.

Where RIPA applies not only must the surveillance be authorised by an authorised officer of the Council but that authorisation must receive Judicial Approval. .

The Corporate Directors and Section 151 Officer are responsible for authorising applications for directed surveillance or the use of a CHIS in respect of the regulatory services for which they are responsible.

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

"for the purpose of preventing or detecting crime or preventing disorder" conduct which constitutes one or more criminal offices and is an offence which is punishable on conviction by a sentence of at least 6 months imprisonment unless it offence is of selling alcohol or tobacco to children under 18"

Authorisation under *RIPA* gives lawful authority to carry out directed surveillance and for the use of a CHIS. Before approving applications, the Authorising Officer must have regard to the necessity and proportionality of the application.

Proportionality means that the action taken must be appropriate, fair and sufficient and that a sledgehammer should not be used to crack a nut. For example, if the evidence can be gained without surveillance then there should be **no authorisation** or, if sufficient evidence can be gained in one surveillance/visit then four must not be taken. Strict compliance with RIPA is imperative. Failure to follow the requirements can amount to unlawfulness on the part of the Council and furthermore, potentially give rise to contravention of rights under Article 8 of the European Convention on Human Rights.

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

There are Home Office Codes of Practice that expand on the information in this guide and copies are available as appendices to this policy, on the Internet and under Policies on the Intranet.

Click here for the hyper link to the Home Office web site.
http://www.homeoffice.gov.uk

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

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 relevant to a question 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".

Deciding when authorisation is required involves making a judgement. Section 1.3 of this guidance gives some examples and Section 1.4 explains the authorisation process. 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 Team.

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).

Teams of 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 Team Manager **must ensure that any "local" guidance does not conflict with this corporate document.**

1.2 DEFINITIONS

What is meant by:

RIPA 2000

RIPA 2000 stands for the Regulation of Investigatory Powers Act 2000.

Surveillance

Surveillance includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication and, for the purposes of *RIPA*, the term persons includes "any organisation and any association or combination of persons", this will include limited companies, partnerships, co-operatives etc;

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

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

Covert Surveillance?

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

If activities are open and not hidden from the persons subject to surveillance, the *RIPA* framework does not apply.

Directed surveillance?

Surveillance is 'Directed' for the purposes of *RIPA* if it is covert, but not intrusive and is undertaken :

a) for the purposes of a specific investigation or a specific operation: and
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. ***This could include the use of an overt CCTV system for a directed and specific covert purpose***.

Intrusive Surveillance?

Intrusive Surveillance is available only to the Police or other law enforcement agencies. Intrusive Surveillance is surveillance undertaken covertly and :

a) is 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) is 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.

Covert Human Intelligence Source (CHIS)

CHIS is defined as a Covert Human Intelligence Source and procedures for the authorisation of a CHIS are set our under Section 29 of RIPA 2000. A CHIS is a person who is required to establish, maintain a personal or other relationship with someone to obtain information in order to assist an investigation. Other relationships can include professional, business or working relationships. A CHIS is therefore the person who acts covertly and passes information to the designated handler.

Authorising Officer

An AO is and employee of Harborough District Council who has received adequate training and has attained a level of competency to be able to provide authorisation. Authorisations within Harborough District Council can only be given by the Corporate Directors and the Section 151 Officer

Investigation Officer (IO)

An investigation Officer is an officer within the Council who is involved in undertaking specific investigation or operation.

Designated Handler

A Designated handler is responsible for directing the day to day activities of the CHIS as well as the security and welfare of the CHIS.

Private Vehicle

Private vehicles are subject to RIPA where any vehicle is used primarily for the private purposes of the person who owns it or for a person who otherwise having right to use it

Necessity

Necessity requires that the covert surveillance takes place when there are no reasonable and effective alternative (overt) means of achieving the desired objective. Please see section 1.4 for further details.

Proportionality

If the activities are necessary then the AO must believe that the activity is proportionate to the likely outcome. The activity will not be proportionate if it is considered excessive in the circumstances of the case, or if the information could have reasonably been sought by other less intrusive means bearing in mind any collateral intrusion caused.

Collateral Intrusion

Collateral Intrusion is where surveillance indirectly intrudes onto the privacy of individuals who are not the direct subject of the surveillance i.e. where innocent bystanders are observed in the course of a surveillance operation. Children are included in this definition.

Residential Premises

Residential Premises are subject to RIPA where premises are being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is occupied or used). Residential accommodation does not include common parts of blocks of flats.

Surveillance Device

Surveillance device means any apparatus designed or adapted for use in surveillance.

Public Authority

Public Authority means any public authority within the meaning of Section 6 Human Rights Act 1998 (Acts of Public Authorities) Courts and tribunals are public authorities.

Human Rights Act

The Human Rights Act 1998 Article 8 provides protection to an individual's right to privacy.

Covert Purpose

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 the purpose behind the relationship.

Private Information

Private information is any information relating to a person's (see the definition in surveillance part a above) private or family life. ***This includes the right to establish and develop relationships with other human beings and activities that are of a business or professional nature.***

For example, if part of an investigation is to observe a member of staff's home to determine their comings and goings then that surveillance would, almost certainly, gather private information, as would surveillance of an individual selling counterfeit goods as the surveillance may provide information about the earnings that the person made from the sales.

Senior Responsible Officer

It is considered good practice for every public authority to appoint a Senior Responsible officer (SRO). The SRO for Harborough District Council is The Head of Legal and Democratic Services (Verina Wenham). The SRO is responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance:
- compliance with Part 2 of the Ac and the Codes:
- engagement with the OSC inspectors when they conduct their inspections where applicable; and
- where necessary, oversight and implementation of post inspection plans approved by the OSC.

Councillors Role

Councillors now have a formal scrutiny role in relation to RIPA. At least once a year they should review the use of RIPA and set the general surveillance policy. They should also consider the internal reports on the use of RIPA on least a quarterly basis to ensure that it is being used consistently as per the councils policy and that the policy remains fit for purpose. It is important to note that councillors should not be involved in making decisions on specific authorisations.

Confidential Material

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 NB1 below)

- "Confidential Personal Information" is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  a) to his/her physical or 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 or unpaid office (see NB2 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:

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

  2)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.

NB 1. Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal adviser is advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation.

NB 2. 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.

1.3 DOES RIPA PART II APPLY TO MY SITUATION?

Is it for the purposes of a specific investigation or a specific operation?

The test is if the surveillance is directed at a known individual or group the provisions of RIPA will cover the investigation. ***If the identity of the individual(s) is not known then this fact should be made clear in the application***.

In respect of other situations, such as CCTV cameras that are readily visible to anyone walking around the area, their use is not governed by RIPA. However**, if the cameras are used as part of an operation to observe a known individual or group it is very likely that RIPA will apply** and an appropriate authorisation will be required. Should an organisation such as the police request direct surveillance then the police authorise the action. The authorisation is then passed to the ***Corporate Directors*** or Section 151 Officer for checking.

Is the surveillance likely to obtain private information about a person?

If it is likely that observations will result in the obtaining of private information about any person, then RIPA may apply.

If in doubt, it is safer to seek authorisation

Is the Surveillance Intrusive?

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the present of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.

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.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

The Council is NOT authorised to carry out intrusive surveillance.

Is the surveillance an immediate response to event or circumstances where it is not reasonably practicable to get authorisation?

The Home Office guidance indicates that this is to take account of an immediate response to something happening during the course of an observer's work, which is unforeseeable. If this occurs, the surveillance will not require prior authorisation.

However, if, as a result of an immediate response, a specific investigation subsequently takes place that investigation will be within the scope of *RIPA.*

1.4 AUTHORISATIONS, RENEWALS AND DURATION UNDER RIPA PART II

1.4.1 The conditions for authorisation

Remember that authorisation must then gain judicial approval.. Once the authorisation has been obtained an application must be made to the Magistrates' court. The Head of Legal and Democratic Services will provide the necessary designation for the application to be made.

The applicant for judicial authorisation need not be legally qualified and it will, in the majority of cases, be the investigating officer who possesses the most detailed knowledge of the case and

the reason why a covert investigation is being sought. The IO will therefore, in the majority of cases, be the most knowledgeable person to both submit and present the application to the Magistrates Court and moreover, answer any questions the court (sitting in private) may have in respect of the application.

Once authorisation is gained from a designated Authorising Officer, the IO should then seek designation from the Head of Legal Services.

The procedure and process for seeking judicial approval is described in detail in the Home Office Guidance of 2012 at Appendix 7. **All applications should follow this guidance.**

Directed Surveillance

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

a) that an authorisation is *necessary* that is, it has to be gained to be able to gather the information needed for the detection or prevention of crime. (Also, see Chapter 2 of the relevant Codes of Practice at Appendix 3).

b) the authorised surveillance is *proportionate* to what is sought to be achieved by carrying it out and that a sledgehammer is not being used to crack a nut. Any surveillance that is carried out must be at the most appropriate level to achieve the objectives of the investigation. (Additional guidance is available in Chapter 2 of the relevant Codes of Practice at Appendix 3). ***The Code of Practice gives 'the person granting the authorisation must believe that 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 the objective in question and must not be arbitrary or unfair'***

An authorisation for directed surveillance under *RIPA* will only be given if the work is:

1) for the purpose of detecting or preventing crime or preventing disorder; **AND**
2) The matter involves a criminal offence punishable by a maximum custodial sentence of six months or more or a related to the underage sale of alcohol or tobacco

The onus is on the people authorising the surveillance activity to satisfy themselves that the action to be taken is necessary and proportionate.

In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. An application form must be completed (see Appendix 2).

See the flowchart in Appendix 1, page 2.

Use of Covert Human Intelligence Sources

The same principles as Directed Surveillance apply in that the application must be authorised and have obtained judicial approval(see paragraph 1.4.1 above). However, the **CRIME THRESHOLD DOES NOT APPLY TO CHIS AUTHORISATION**. The conduct authorised by a CHIS authorisation is any conduct that:

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

b) relates to the person who is specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and

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

In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. An application form must be completed.

See the flowchart in Appendix 1, page 3.

1.4.2 Provisions of RIPA PART II

Authorisations must be in writing. Standard forms are available from the RIPA Public site (which can be found at Appendix 2 or by accessing the W: drive, double clicking Public, then Criminal & other investigation (Forms), then RIPA but officers must ensure that the circumstances of each case are accurately reflected on the application form.

The practical effect of the requirement for approval by a Magistrate is that oral authorisations are no longer available.

Directed surveillance and the use of a CHIS will be applied for on the relevant forms, even if they relate to the same surveillance target.

Authorisations **must** be cancelled as soon as they are no longer required, and, in any event, on or before the expiry date of the authorisation.

Authorisations only last, if not renewed:

- Any authorisation granted or renewed orally, (or by a person whose authorisation was confirmed to urgent cases) expire after 72 hours, this period beginning with the time of the last grant or renewal;

- A written authorisation to use a CHIS expires after 12 months from the date of judicial approval

- in all other cases (i.e. directed surveillance) 3 months less one day from the date of judicial approval.

Any person entitled to grant a new authorisation, as described above, can renew an existing authorisation, on the same terms as the original authorisation, at any time before the original ceases to have effect.

A CHIS application should not be renewed unless a thorough review has been carried out and the authorising officer has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

1.4.3 Factors to Consider

General

Any person giving an authorisation should satisfy themselves, based on the information in the application and their knowledge of the service that:

- the authorisation is necessary
- the surveillance is proportionate to what it seeks to achieve.

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

An application for an authorisation **must include an assessment of the risk of any collateral intrusion or interference.** The authorising officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

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

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

The keeper of the central register will inform the Investigating officers of the review time. **The *Authorising* Officer is responsible for ensuring that approvals, reviews, renewals and recommendations for cancellation are made and timely.**

Directed surveillance away from the subject's workplace or in a public area

The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance at his/her home, or where there are special sensitivities. Care must be exercised, particularly in relation to residential premises, to avoid carrying out any surveillance that may be deemed to fall under the definition of Intrusive Surveillance (because a local authority is not empowered to undertake intrusive surveillance).

Spiritual Counselling

No operations should 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 Material

RIPA does not provide any special protection for confidential material (see the definition in Appendix 1). Nevertheless, such material is particularly sensitive, and is subject to additional safeguard under this code. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the

source should be subject to special authorisation by the Head of Paid Service. Where the authorisation is for the obtaining of legally privileged information it can **ONLY** be given by an ordinary Surveillance Commissioner (i.e. one of the commissioners at the Office of Surveillance Commissioners) and **NOT** by an officer of the Council.

In general, any application for an authorisation that 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.

The following general principles apply to confidential material acquired under 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 Head of Legal and Democratic Services before further dissemination takes place;

- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Head of Legal and Democratic Services) is satisfied that it is necessary 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. Any material of this nature will be reviewed on a monthly basis by the Team Manager.

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

Combined authorisations

A single authorisation may combine two or more different authorisations under RIPA (but cannot include an authorisation for intrusive surveillance activity).

In cases of joint working with other agencies on the same operation, authority for directed surveillance by a Housing Benefit Investigator working with a Benefits Agency investigator must be obtained from the Council's authorising officers. Authority can be granted by the authorising officer of another body for the actions of Council staff and vice versa ***but the wording of the application must be precise. Consult with the Legal Services team for advice prior to considering this course of action.***

Handling and disclosure of the products of surveillance

Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described above.

The Authorising Officer should retain RIPA related documents for a period of 3 years. However, 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.

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

obtained by surveillance is wholly unrelated to a criminal or other investigation, or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer. ***The Authorising Officer must ensure that the Cancellation form is complete in accordance with the relevant codes.***

Material obtained through the proper use of the RIPA authorisation procedures can be used for relevant Council purposes. However, the transfer of such information outside the Council, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances and should always only occur following consideration of the appropriate Data Protection legislation.

The Use of Covert Human Intelligence Sources (CHIS)

It is not the Council's normal practice to seek, cultivate or develop a relationship with a potential external or professional source, although this action is not precluded if it meets the RIPA conditions. It is possible that a Council employee may be used as a CHIS and nothing in RIPA prevents material obtained by an employee acting as a CHIS being used as evidence in Court proceedings.

The Authorising Officer must consider the safety and welfare of an employee acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out **before** authorisation is given. (See appendix 1 for risk assessment forms). The safety and welfare of the ***individua***l, even after cancellation of the authorisation, should be considered from the very outset.

Before authorising the use of a CHIS (known as a source), a risk assessment must be carried out. Attention is drawn to section 4 of the Code of Practice in the use of a CHIS. The Authority must put in place, before authorisation, a system to manage the source. A person must be appointed to oversee the use of the source. That person will be called the ***Controller*** of the source. There must also be a person appointed to take responsibility for the day to day activities of the source, this will include the recording of the information gained. That person will be called the Handler of the source. (See authorisation flowchart in Appendix 1)

The authorising officer must ensure that, as far as is possible, measures are taken to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

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.

Confidential material

RIPA does not provide any special protection for confidential material. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under the relevant Home Office Code. In cases where the likely consequence of the conduct of a CHIS or a directed surveillance operation would be for any person to acquire knowledge of confidential material, the deployment of the CHIS or the carrying out of the surveillance should be subject to special authorisation by the Head of Paid Service.

Any application for an authorisation that 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.

Register of Authorisations

The Head of Legal and Democratic Services is responsible for maintaining a central register of authorisations. The Legal Team will maintain the register, which will record the date of the authorisation, the name of the authorising officer and the location of the file where the authorised application will be retained. The Officer who has authorised the application must contact the Legal Team to provide them with the specified information and to obtain a reference number for the authorisation. This must be done on the day that the application is authorised. The Authorising Officer must then ensure that the authorised application is filed in the location notified to the Legal Team. The original will be kept in the Central register. The ***Corporate Directors or Section 151 Officer*** permitted to authorise applications under *RIPA* will ensure that their Team maintains appropriate files for all applications, approvals and cancellations. Cancellations must be attached to the relevant authorised applications.

RIPA PART I CHAPTER II –
THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

2.1 INTRODUCTION

Part I Chapter II (sections 21 – 25 of RIPA) came into force on 5th January 2004. It regulates the acquisition and disclosure of communications data. It provides powers for the Council to gain communications information when carrying out investigations. It also regulates information previously gained without regulations, which now has to be authorised.

The process is similar to that of the authorisation of directed surveillance and CHIS, but has extra provisions and processes.

The purpose of the introduction is the same, that is, to protect people's human rights. The effect of not gaining authorisation when needed is the same. The Council leaves itself open to a challenge under the Human Rights Act 1998 and the evidence gained without authorisation may not be admissible in court.

RIPA specifies that the only purpose for which the Council can gather communication data is in the:

'Prevention and detection of crime or preventing disorder'

There is a Code of Practice which has been supplemented by guidance on the effect of changes to RIPA made by the Protection of Freedoms Act 2012.

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

The Code does not have the force of Statute but are admissible in evidence in any criminal and civil proceedings.

2.2 WHAT IS COMMUNICATIONS DATA?

The definition of communications data includes information relating to the use of a communications service but it does not include the contents of the communication itself. It is broadly split into 3 categories:

- Traffic data – where a communication was made from, to who and when
- Service data – the use made of a service by any person e.g. itemised telephone records
- Subscriber data – any other information held or obtained by an operator on a person they provided a service to.

This Council is restricted to subscriber and service use data and even then only for the purpose of preventing or detecting crime and disorder. For example a benefit fraud investigator may be able to get access to an alleged fraudster's mobile phone bills.

The word 'data' in relation to a postal item means anything written on the outside such as an address. Officers at the Council have previously been able to apply for the new address of a person that they were investigating, that is the re direction details. A request form was completed and the post office supplied the information. This activity is now regulated and authorisation needs to be gained.

THE CODE DOES NOT COVER THE INTERCEPTION OF COMMUNICATIONS (IE THE CONTENTS OF ANY COMMUNICATIONS INCLUDING THE CONTENT OF AN E-MAIL, OR INTERACTION WITH WEB SITES).

2.3 AUTHORISATIONS, NOTICES, RENEWALS AND DURATION

2.3.1 AUTHORISATIONS AND NOTICES

The Code states that a 'designated person', must decide whether authorisation is necessary and proportionate to the action to be taken. The designated person is in effect the Authorising Officer. The designated persons at this Council are the ***Corporate Directors and the Section 151 Officer***

There are two ways to authorise access to communications data.

(a) Authorisation under 22(3). This allows the authority to collect the data itself. This 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 relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data; or

(b) By a notice under section 22(4). A notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority.

The designated person decides whether or not an authorisation should be granted.

The designated person must take account of the following points when deciding whether to authorise the application or not.

- Is the accessing of data for the prevention or detection of crime or disorder?
- Why is obtaining the data necessary for that purpose?
- Is obtaining access to the data by the conduct authorised proportionate to what is being sort to be achieved? That is what conduct are you authorising and is it proportionate?
- Is the accessing of the data likely to result in collateral intrusion? If so, is the access still justified?
- Is any urgent time scale justified?

The designated person will make a decision whether to grant the authorisation based upon the application made. The application form is at Appendix 2. The application form should subsequently record whether or not the application was approved or not, by whom and the date. **A copy of the application must be kept by the officer until it has been inspected by the Commissioner.**

If the application is authorised by a designated Authorising Officer, it will then be necessary for an application for Judicial Approval to be made.

Due to the nature of the role of the SPoC, for applications relating to communications data, the Head of Legal and Democratic Services will designate the SPOC officer to be the applicant for the purposes of making and presenting the application to the magistrates. **The SPoC must not acquire the data via a communications service provider (CSP) or via automated systems until the order approving the authorisation has been granted.** Once granted, the notice needs to be served. The notice is served upon the postal or telecommunications officer only.

The application form and the authorisation itself are not served upon the holder of the communications data. The authorisation and notice are in the standard form and are at Appendix 2.

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

2.3.2 PROVISIONS OF RIPA

Single Point Of Contact (SPOC)

Notices and authorisations for communications data should be channelled through a SPOC. The Code states that this is to provide an effective system in that the SPOC will deal with the postal or telecommunications operator on a regular basis. Matthew Bradford Service Manager – Contracted Services has been allocated the role of the SPOC. The SPOC will advise the Authorising Officer/designated person on whether an authorisation and/ or notice is appropriate.

The single point of contact should be in a position to:

- Where appropriate, assess whether access to communications data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and designated persons on the practicalities of accessing different types of communications data from different postal or telecommunications operators;
- Advise applicants and designated persons on whether communications data falls under section 21(4)(a), (b) or (c) of the Act. That is traffic, service or subscriber data;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the telecommunications operator.

Oral Authority

This route is **NOT** available to the Council.

Duration

Authorisations and notices will only be valid for one month beginning from the date on which judicial approval is granted or notice given. If the information can be collected in a shorter time period then that should be specified. This would accord with the proportionality element of the decision making.

The postal or telecommunications operator need only comply with the request if it is reasonably practicable to do so.

Renewal

An authorisation or notice can be renewed at any point during the month that it is valid by following the same procedure as in obtaining a fresh authorisation.

Cancellations

The duty to cancel falls on the designated person who authorised it. The notice shall be cancelled as soon as it is no longer necessary or is no longer proportionate to what is being sort to be achieved.

Authorisations should also be cancelled.

In the case of a section 22(4) notice, the postal or communications operator shall be informed of the cancellation.

Retention

Applications, authorisations and notices will be retained by the authority until they have been audited by the Commissioner. The authority should also keep a record of the dates that the notices and authorisations were started and cancelled. A copy of each form should be kept by the investigating Team and the originals kept in the Central Register. Is shall be the responsibility of the designated person to ensure that the records are accurate and kept up to date.

Combined Authorisations

Applications for communications data may only be made by persons in the same authority as a designated person. There cannot, therefore, be any combined authorisations.

Errors

Where any errors have occurred in the granting of authorisations or the giving of notices, a record should be kept and a report and explanation sent to the Commissioner as soon as practical.

3 BENEFITS OF OBTAINING AUTHORISATIONS UNDER RIPA

Authorisation of surveillance, human intelligence sources and the acquisition and disclosure of communications data.

RIPA states that:

> "if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be "lawful for all purposes".

Failure to comply with the requirements of RIPA may render any evidence you place before the courts subject to challenge in respect of the processes used to obtain the evidence (s78 Police and Criminal Evidence Act 1984).

RIPA 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 an authorisation; and

b)is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

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).

4 SCRUTINY AND TRIBUNAL

RIPA set up the Office of the Surveillance Commissioner to regulate the conduct of public bodies and to monitor their compliance with *RIPA*. The Chief Surveillance Commissioner will keep under review, among other things, the exercise and performance of duties, imposed in *RIPA* by the persons on whom those duties are conferred or imposed. This includes authorising directed surveillance and the use of covert human intelligence sources.

A tribunal has been established to consider and determine complaints made under *RIPA* if it is the appropriate forum. Persons aggrieved by conduct, e.g. directed surveillance, can make complaints. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that period.

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. The Council is, however, under a duty to disclose or provide to the tribunal all documents they require if:

- A Council officer has granted any authorisation under RIPA.
- Council employees have engaged in any conduct as a result of such authorisation.
- A disclosure notice requirement is given

APPENDIX 1 – Process Flowcharts

- **Surveillance summary**
- **Directed surveillance**
- **Covert human intelligence source**
- **Authorisation Flowchart**
- **Risk assessment forms**

SURVEILLANCE SUMMARY

Is an investigative technique such as surveillance or undercover officer being considered?

NO

YES

Can the conduct amount to a crime within a possible prison sentence of at least 6 months?

NO

Will the operation be covert?

NO

YES

Is the surveillance carried out in relation to anything taking place on any residential premise or in any private vehicle?

YES → Possible INTRUSIVE surveillance (not within the Council's powers).

NO

Will any information obtained be of the same detail as you would expect from actually being on the premises or in the vehicle

YES → Possible INTRUSIVE surveillance (not within the Council's powers

NO

Is the operation likely to reveal private information about any person?

YES → Possible DIRECTED surveillance
See flowchart (Page 2)

NO

Will the operation involve someone acting 'undercover'?

YES → Possible Covert Human Intelligence Source (CHIS)
See flowchart (Page 3)

NO

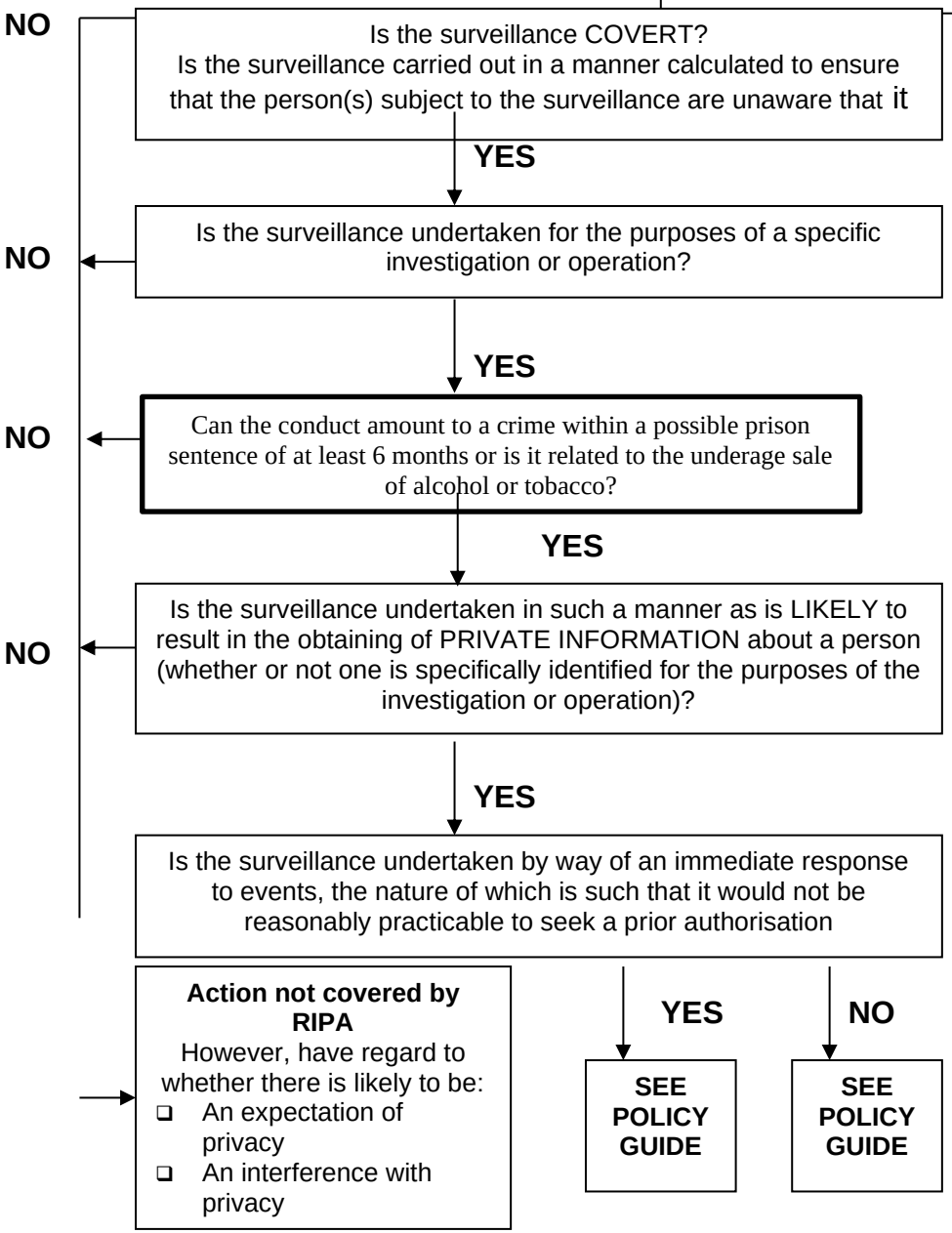
Action not covered by RIPA

However, have regard to whether there is likely to be:

- an expectation of privacy, or
- an interference with privacy

NB A Magistrate must approve

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

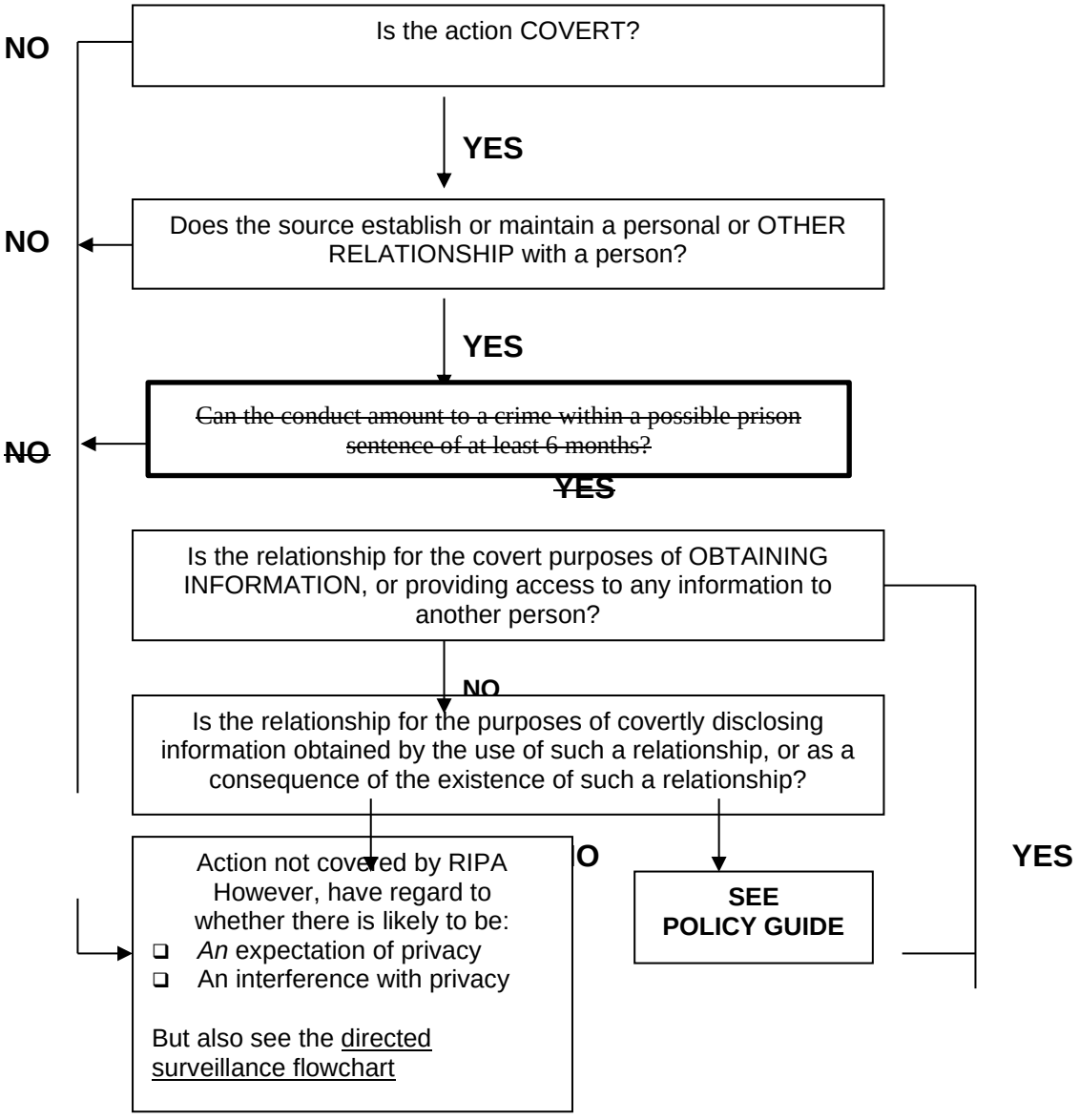
PRIVATE INFORMATION see Section 26(10) RIPA in relation to a person, includes any information relating to his private or family life.
'Private Information' should be given a wide interpretation and should not be restricted to what might be considered to be 'secret' or 'personal' information. Information 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

NB. A Magistrate must approve the authorisation

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 is 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.

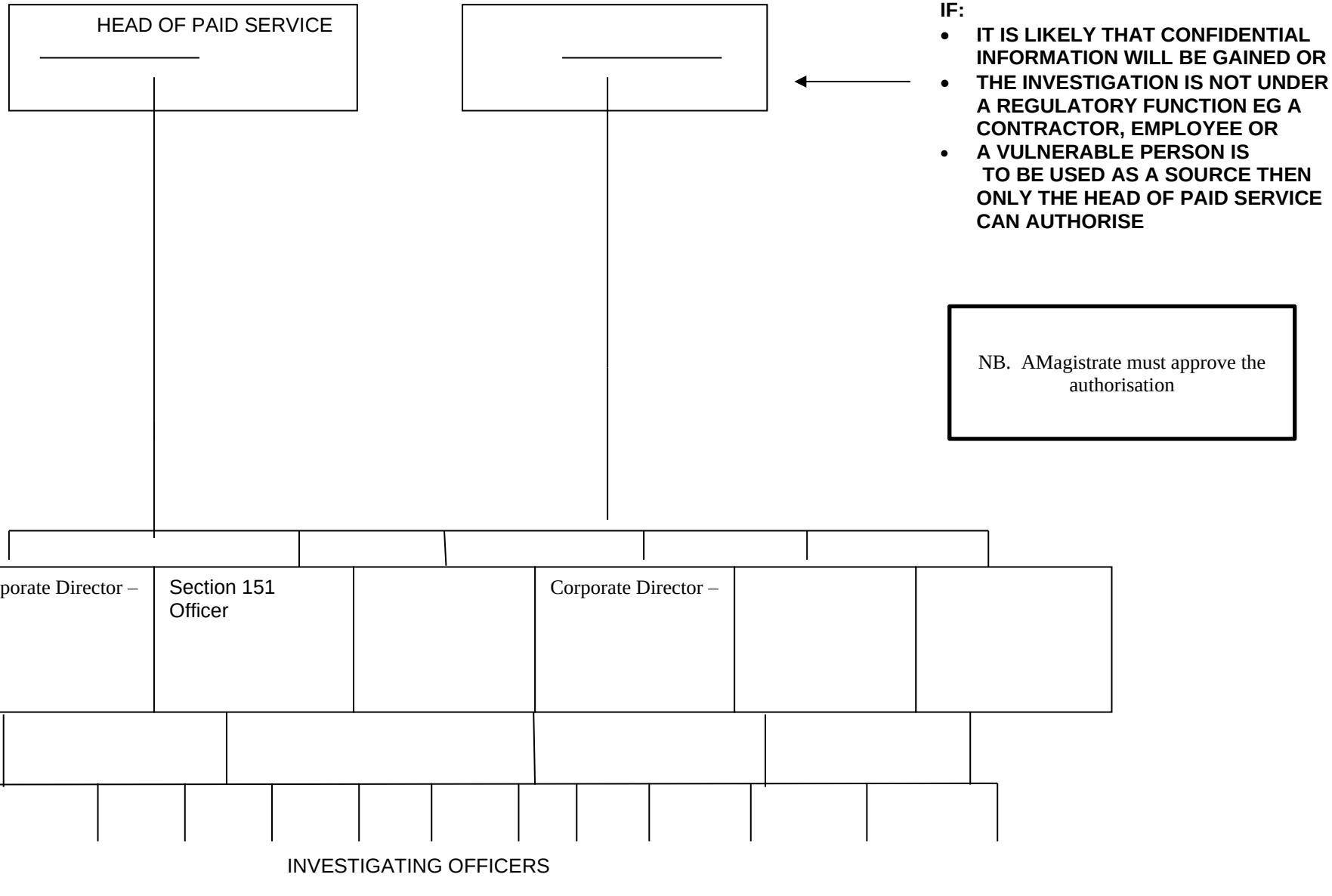
For further interpretation see Sections 48 & 81 RIPA, including Explanatory Notes to RIPA & Codes of Practice on Covert Surveillance & Use of a CHIS.

NB. A Magistrate must approve the authorisation

AUTHORISATION FLOWCHART

OFFICERS
RESPONSIBLE FOR THE RISK ASSESSMENT OF A CHIS

WHO CAN PROVIDE
AUTHORISATION UNDER RIPA



SITE:	Harborough D.C	**TASK BEING ASSESSED**	DATE:	00-00-20
AREA:	**Test page**	**Type item to be assessed.**	RECORD NO:	

No:	TASK/ACTIVITY	NO OF P.A.R.	FREQ. OF EXP.	ASSOCIATED HAZZARDS	EXISTING CONTROLS	L	S	RES RISK FACT	ACTIONS TO ELIMINATE/CONTROL	WHO IS RESPONSIBLE & WHEN	RES RISK FACT
1											
2									r		
3											
4									. .		

5											

GENERAL RISK ASSESSMENT – GUIDANCE NOTES

NUMBER OF PEOPLE AT RISK	
1-2 PEOPLE	1
3-7 PEOPLE	2
8-15 PEOPLE	4
16-50 PEOPLE	8
12-50 PEOPLE	12

FREQUENCY OF EXPOSURE

1 INFREQUENT
2 ANNUALLY
3 MONTHLY
4 WEEKLY
5 DAILY
6 HOURLY
7 CONSTANTLY

LEGAL STANDARD

COSHH WORK EQUIPMENT
NOISE MANUAL HANDLING
SIGNS ELECTRICITY
FIRE ASBESTOS
LEAD FIRST AID
PPE DSE

RESIDUAL RISK FACTOR

LIKELIHOOD x SEVERITY
= HIGH, MED OR LOW

HAZARD PROMPT LIST – NON EXHAUSTIVE

Falls from height
Falls of objects from a height
Walking on slippery/uneven floors
Manual handling
Use of machines
Operation of vehicles
Fire
Mechanical lifting operations
High Noise levels
Biological agents
Ionising radiation
Vibration
Use of hand tools
Adverse Weather
Stacking
Moving Machinery/Parts
Behaviour/attitude

Excavation work
Stored energy
Flammable, explosive materials
Chemicals/dust
Hot/cold surfaces
Lighting
Confined spaces
Housekeeping
Repetitive Movement
Static posture
Cleaning Operations
Maintenance
Electricity
Compressed air
Violence
Stress

LIKELIHOOD						
	5					
	4					
	3					
	2			1 MEDIUM		
	1	LOW				
		1	2	3	4	5
		SEVERITY				

1 - 4 NO ACTION 5 – 9 ACTION MAY BE REQUIRED 10 – 25 ACTION REQUIRED	PAGE 3

APPENDIX 2

Application for Directed Surveillance
Review Directed Surveillance
Renewal Directed Surveillance
Cancellation Directed Surveillance
Application for CHIS
Review of CHIS
Renewal of CHIS
Cancellation of CHIS
Application for Communications Data
Communication Data notice
SPoC Report
SPoC Log Sheet
Judicial Approval Order form

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Public Authority *(including address)*	

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

Details of review:

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

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

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Part II of the Regulation of Investigatory Powers Act 2000

Renewal of a Directed Surveillance Authorisation

Public Authority *(including full address)*	

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

Details of renewal:

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

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

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

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

Details of cancellation:

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

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

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

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

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

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

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

Review of a Covert Human Intelligence Source (CHIS) Authorisation

Public Authority *(including full address)*	

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

Review Number	

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

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

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

(Please attach the original authorisation)

Public Authority *(including full address)*	

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

Details of renewal:

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

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

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

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

Public Authority *(including full address)*	

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

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Insert name of your public authority here

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000

Application for Communications Data

1) Applicant's Name		**4) Unique Reference Number**	
2) Office, Rank or Position		**5) Applicant's Telephone Number.**	
3) Applicant's Email Address		**6) Applicant's Fax Number**	

7) Operation Name (if applicable)		**8) STATUTORY PURPOSE**
		Click here for options:-

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

10) NECESSITY **State the nature of the investigation or operation and how it relates to a purpose at question 8** *Give a short explanation of the crime (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together.*

11) PROPORTIONALITY **State why obtaining the communications data is proportionate to what you are seeking to achieve** *Outline what is expected to be achieved from obtaining the data and explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy? Explain why you have requested the specific date/time periods i.e. how these are proportionate.*

12) COLLATERAL INTRUSION *Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances* *If you have identified any meaningful degree of collateral intrusion, explain what it is.*

13) TIMESCALE **Identify and explain the timescale within which the data is required**	

14) APPLICANT **I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data**			
Applicant's Signature		**Date**	

(**a**) 2000 c. 23.

(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Insert name of your public authority

NOTICE

Section 22(4) of the Regulation of Investigatory Powers

Where it appears to the designated person that a CSP is or may be in possession of, or be capable of obtaining, any
may, by notice require the CSP -

(a) if the CSP is not already in possession of the data, to obtain the data; and

(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

S. 22(6) - It is the duty of the CSP to comply with any notice given to him under subsection (4).

Other SPoC Reference*		Unique Reference Number of Notice	
Details of the CSP	**Name of the CSP** **Address of CSP** **For attention of**		
Statutory Purpose	**Click here for options:-**		
Designated Person Giving Notice This Notice is valid for one month when given by the Designated Person	**Name of the DP** **Office, rank or position** **Date Notice given** **and if appropriate the time**		
Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought.	**Data applied for** **Time period (if applicable)**		
URGENT (DCG Grade 1 or 2) may only be initiated by SPoC and will require liaison with CSP staff. DCG Grade 3 – SPoC may indicate any specific or critical time issues such as bail dates, court dates, persons in police custody, specific line of investigation in serious crime (S.81(2) RIPA) investigation and the acquisition of data will directly assist in the prevention or detection of the crime.	**DCG Grading Scheme** **Click here for options:-** **Grade 3: If, and only if there is a specific or critical time issue state the 'target date' for the disclosure of the data** **Explain the reason for the setting of a target date** **Comment:** Ordinarily all requirements are Grade 3 and will be dealt with in date order when received by the CSP. DCG has requested the IOCCO Inspectors to make appropriate comment on the use of the grading scheme during their inspections of law enforcement agencies		
Specify the manner in which the data should be disclosed	**Click here for options:-**		
SPoC Office Contact Details and Address[1] If there is a specific or critical time issue indicated or the matter is DCG Grade 1 or 2 URGENT then the Accredited SPoC contact details MUST be completed	**TEL** **FAX** **EMAIL** **POSTAL** **Name of Accredited SPoC** **Mob TEL** **Reminder:** If you have requested a "24/7" response from the CSP make sure you supply sufficient contact details so that you and your SPoC colleagues can be easily contacted		
Date Notice served **and if appropriate the time**			

[1] CSPs must ensure the data is returned to a verified SPoC email or fax number.
For information about how a CSP may verify the identity of a SPoC by use of the SPoC PIN list, contact commsdata@

October 2007

(**a**) 2000 c. 23.

(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

HARBOROUGH DISTRICT COUNCIL

SPOC OFFICER REPORT

SPOC Ref. No.		**Application Ref. No.**	

Estimate of cost to obtain the data (£)		• **21 (4)(b)**	• **21(4)(c)**

Adverse Impact on CSP?	**Yes**	•	**No**	•	**Details**	
Adverse Impact on Public Authority?	**Yes**	•	**No**	•	**Details**	

To be completed by SPOC					
URN of Notice or Authorisation	**Designate Person**	**Telephone Number/Other Requested (Subscriber/Account details) or Service Required. Date and Time Period From/To**	**Communication Service Provider**	**Notice S22 (4) Specify the conduct required to retrieve the data** **1. Email** **2. Fax** **3. Post** **4. Personal Delivery** **5. Already verbally approved by Designated Person and Data obtained from CSP**	Authorisation S22 (3) **Specify the conduct required to retrieve the data** **1. Via the Automated system** **2. By members of the Designated persons LEA visiting the CSP and retrieving the data themselves** **3. Already verbally approved by Designated Person and Data obtained from CSP**
1.					
2.					
3.					
4.					
5.					
Is this application reasonably practicable and feasible for the CSP?					
• **Yes**			• **No Please provide reason**		

Will this request produce any excess data, which falls outside the parameters of the application?		**Other comments, information for Designated Person**
• **No** • **Yes Please provide details**		

SPOC Officer Name		**Time and Date**	

(**a**) 2000 c. 23.

(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

HARBOROUGH DISTRICT COUNCIL

SPOC LOG SHEET

TELEPHONE NUMBER/OTHER ----------

SPOC Ref. No.		**Application Ref. No.**	

URN of Notice or Authorisation (if appropriate)	Summary of Enquiry Time and Date CSP or other person whom SPOC spoke to Result (If appropriate who was the information passed onto and in what format and at what time and date) or any other information which may be relevant to this case	**1 Name of SPOC**

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

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:.....

(**a**) 2000 c. 23.

(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Appendix 3

Statutory Instrument 2010 480

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

STATUTORY INSTRUMENTS

2010 No. 480

INVESTIGATORY POWERS

The Regulation of Investigatory Powers (Communications Data) Order 2010

Made - - - - 25th February 2010
Coming into force - - 6th April 2010

This Order is made in exercise of the powers conferred on the Secretary of State by sections 22(2)(h), 25(2) and (3) and 78(5) of the Regulation of Investigatory Powers Act 2000(1), together with paragraph (g) of the definition of "relevant public authority" in section 25(1) of that Act.

In accordance with sections 22(9) and 25(5) of that Act, a draft of this Order was laid before Parliament and approved by a resolution of each House of Parliament.

Accordingly, the Secretary of State makes the following Order—

Citation, commencement and interpretation

1.—(1) This Order may be cited as the Regulation of Investigatory Powers (Communications Data) Order 2010 and shall come into force on 6th April 2010.

(2) In this Order—

"the Act" means the Regulation of Investigatory Powers Act 2000;

"authorisation" means an authorisation under section 22(3) of that Act; and

"notice" means a notice under section 22(4) of that Act.

Additional purposes of section 22(2) of the Act

2. The following additional purposes are specified for the purposes of section 22(2) of the Act (to the extent that they do not fall within paragraphs (a) to (g) of that provision)—

(a) to assist investigations into alleged miscarriages of justice;

(b) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—

(i) to assist in identifying P, or

(1) 2000 c.23; section 25 has been amended by paragraph 135 of Schedule 4 to the Serious Organised Crime and Police Act 2005 (c.15).

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

APPENDIX 4

Statutory Instrument 2010 521

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

STATUTORY INSTRUMENTS

2010 No. 521

INVESTIGATORY POWERS

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010

Made - - - - 25th February 2010
Coming into force - - 6th April 2010

This Order is made in exercise of the powers conferred on the Secretary of State by sections 30(1), (3), (5) and (6) and 78(5) of the Regulation of Investigatory Powers Act 2000(**1**).

In accordance with section 30(7) of that Act, a draft of this Order was laid before Parliament and approved by a resolution of each House of Parliament.

Accordingly, the Secretary of State makes the following Order—

Citation, commencement and interpretation

1.—(1) This Order may be cited as the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and shall come into force on 6th April 2010.

(2) In this Order "the Act" means the Regulation of Investigatory Powers Act 2000.

Amendment of Parts 1 and 2 of Schedule 1 to the Act

2.—(1) Schedule 1 to the Act (relevant public authorities) is amended as follows.

(2) In Part 1 (relevant public authorities for the purposes of sections 28 and 29) omit—

(a) paragraph 4A (the force comprising the special constables appointed under section 79 of the Harbours, Docks and Piers Clauses Act 1847(**2**) on the nomination of the Dover Harbour Board)(**3**),

(b) paragraph 10 (the Ministry of Defence),

(c) paragraph 15B (the Department for Work and Pensions)(**4**),

(d) paragraph 20D (the Postal Services Commission)(**5**), and

(1) 2000 c.23.
(2) 1847 c.27 (10 & 11 Vict.).
(3) Inserted by S.I 2005/1084.
(4) Inserted by S.I 2002/1397.
(5) Inserted by S.I. 2003/3171.

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

APPENDIX 5

Statutory Instrument 2012 1500

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

STATUTORY INSTRUMENTS

2012 No. 1500

INVESTIGATORY POWERS, ENGLAND AND WALES

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012

Made - - - -	*11th June 2012*
Laid before Parliament	*14th June 2012*
Coming into force - -	*1st November 2012*

This Order is made in exercise of the powers conferred on the Secretary of State by sections 30(3) and (6) and 78(5) of the Regulation of Investigatory Powers Act 2000(**1**).

Citation and commencement

1. This Order may be cited as the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 and shall come into force on 1st November 2012.

Amendment of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010

2.—(1) The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010(**2**) is amended as follows.

(2) In article 3(2) (prescribed offices, ranks and positions with relevant public authorities) for "articles 5 to 7" substitute "articles 5 to 7A".

(3) In article 4(1) (additional offices, ranks and positions prescribed for urgent cases) for "articles 5 to 7" substitute "articles 5 to 7A".

(4) After article 7 (restrictions on the granting of authorisations) insert—

"**7A.**—(1) An individual holding an office, rank or position with any county council or district council in England, a London borough council, the Common Council of the City of

(**1**) 2000 c.23.
(**2**) S.I. 2010/521, to which there are amendments not relevant to this Order.

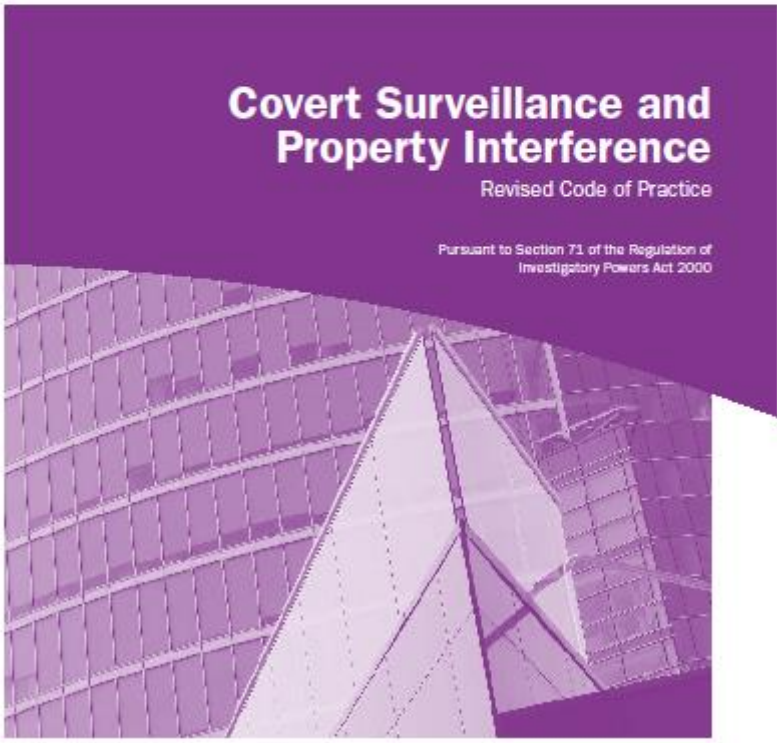
(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

APPENDIX 6 -

Code of Practice for Covert Surveillance and property interference 2010

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Home Office



(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

APPENDIX 7

RIPA Home Office Guidance 2012

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.

Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance

Home Office

October 2012

(**a**) 2000 c. 23.
(**b**) 1997 c.50; section 91(1) has been amended by S.I. 1999/1747.