MELTON BOROUGH COUNCIL

POLICY AND GUIDANCE

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 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 Public Bodies defined in *RIPA* include Local Authorities and, therefore, Melton Borough 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
- 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 these are reproduced at Appendix 3, Appendix 4 and Appendix 5. They are also available on the *RIPA* section of the Policies part of the Council's Intranet. This can be found by accessing the Melton Borough Council 'Q' Drive under 17 Legal Services\Advice\RIPA\RIPA Training 2010. 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.

The Chief Executive, Strategic Directors, Head of Communities and Head of Regulatory Services 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 of preventing disorder;"

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 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. But, once obtained, the authorisation helps to protect 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).

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 on the Internet and under Policies on the Intranet.

Covert Surveillance:

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 Survelliance 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 Melton Borough Council who has received adequate training and has attained a level of competency to be able to provide authorisation. Authorisations within Melton Borough Council can only be given by the Chief Executive Officer, Strategic Directors, Head of Communities and Head of Regulatory Services.

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 Melton Borough Council is The Solicitor to the Council (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 Surveliiance:
- compliance with Part 2 of the Ac and the Codes:
- engagement with the OSC inspectors when they conduct their inspections where applicable and;; 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:
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.

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.

Any authorisation that are subject to legal privilege should always comply with SI 2010 /123 a copy of which can be found at Appendix 7.

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. The CCTV policy is at Appendix 6. Should an organisation such as the police request direct surveillance then the police authorise the action. The authorisation is then passed to the relevant Strategic Director and the Control Centre Manager 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.

<u>If in doubt, it is safer to seek authorisation</u>

Is the Surveillance Intrusive?

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on <u>residential</u> premises or any <u>private</u> 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

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 under *RIPA* will only be given if the work is:

"for the purpose of preventing or detecting crime or of preventing disorder;"

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 the flowchart in Appendix 1, page 2.

Use of Covert Human Intelligence Sources

The same principles as Directed Surveillance apply. (see paragraph 1.4.1 above) 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

For *urgent* grants or renewals, oral authorisations are acceptable, but should be followed up with a written application as soon as possible thereafter. Urgent grants are those where authorisation would be needed but the circumstances are such that if a grant was waited for then the time for the gathering of the information would have passed and the opportunity missed. See form at Appendix 2. In all other cases, authorisations must be in writing. Standard forms are available from the RIPA Public site (which can be found by accessing the Q Drive under 17 Legal Services\Advice\RIPA\RIPA Training 2010) but officers must ensure that the circumstances of each case are accurately reflected on the application form.

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 last renewal or

- in all other cases (i.e. directed surveillance) 3 months from the date of their grant or latest renewal.

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.

The benefits of obtaining an authorisation are described in section 3 below.

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 Chief Executive.

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 Services before further dissemination takes place;

- Confidential material should be disseminated only where an appropriate officer (having sought advice from The Solicitor to the Council) 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 cannot be granted by the authorising officer of another body for the actions of Council staff and vice versa.

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 individual 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 individual, 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 Chief Executive.

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 Solicitor to the Council 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. A Director who is 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.

2 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 draft Code of Practice. It can be found at Appendix 5, on the Q Drive under 17 Legal Services\Advice\RIPA\RIPA Training 2010 and as an Appendix to the Policy and Guidance on the Intranet.

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

The Code does not have the force of Statute but are admissable 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 Chief Executive Officer, Strategic Directors, Head of Communities and Head of Regulatory Services.

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.

(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 and the notice needs to be served, then only the notice is served upon the postal or telecommunications officer.
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. Jackie McSporran 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

An oral application and approval can only be made on an urgent basis for the purpose set out in 22(2)(g) of the Act. That is

> "for the purpose, in emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health".

That is not a purpose under which the council is able to collect communications data and therefore oral authorisations are not possible.

Duration

Authorisations and notices will only be valid for one month beginning from when it was granted. 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".

However, the opposite is not true – i.e. if you do not obtain *RIPA* authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits and you may have to justify infringing a person's Human Rights and any evidence you place before the courts may be 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

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)

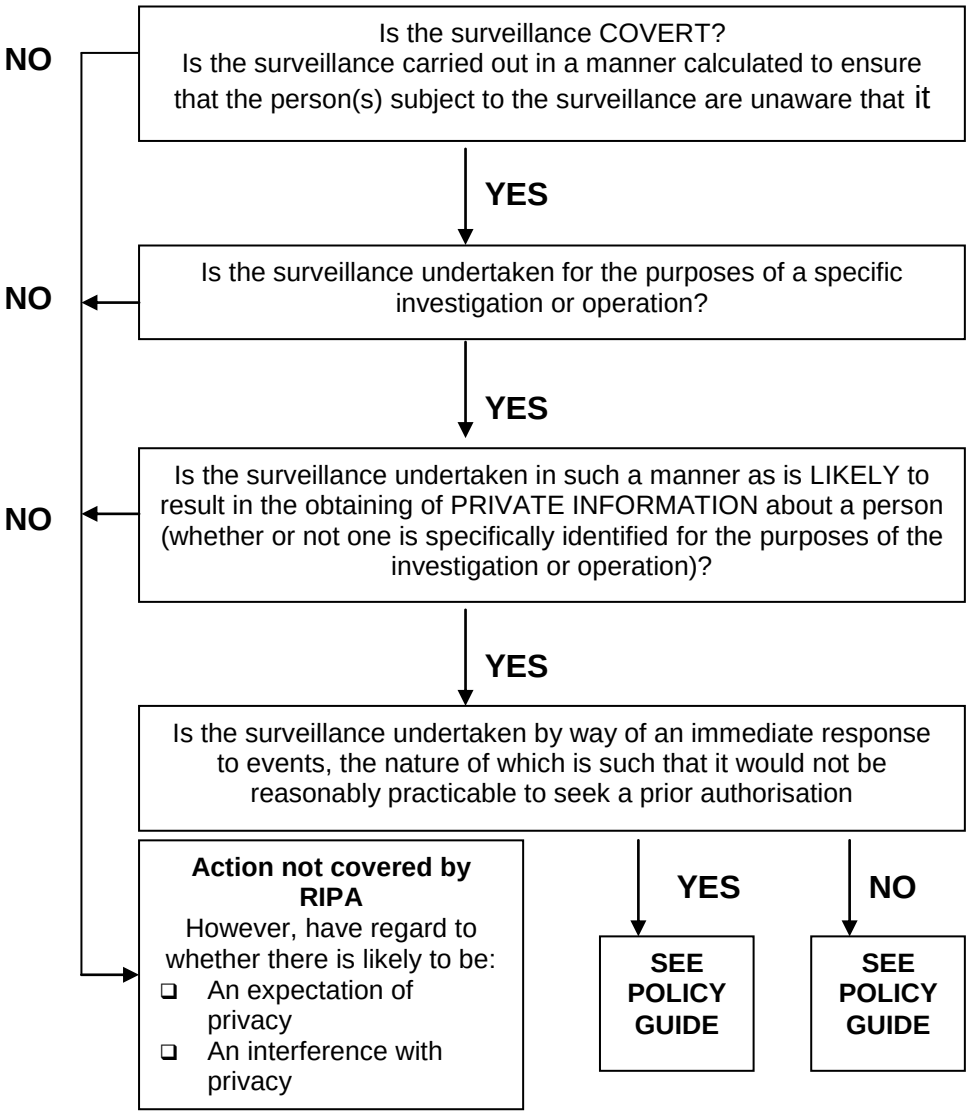
NO

Action not covered by RIPA

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

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

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

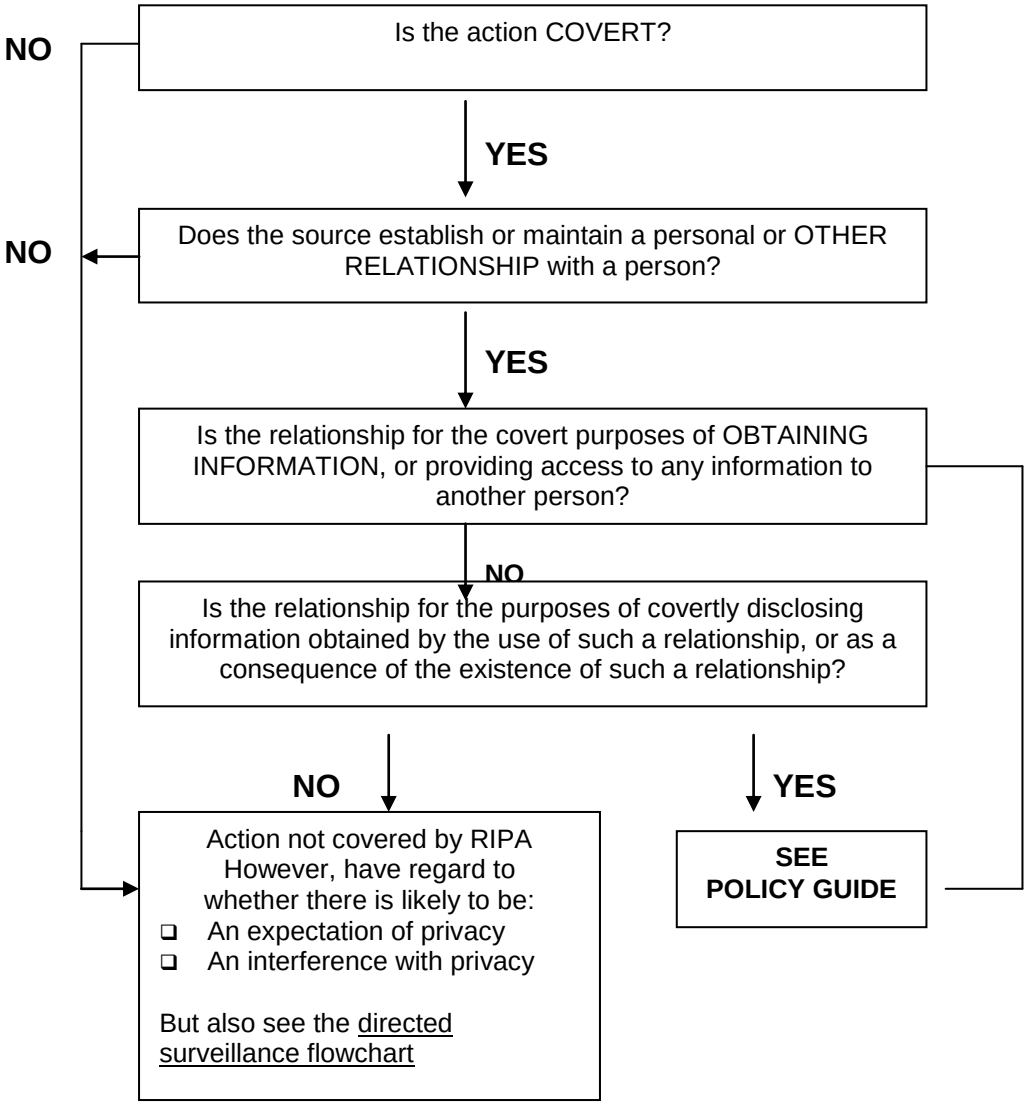
PERSON see Section 81(1) RIPA. Includes any organisation and any association or combination of persons

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 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.

AUTHORISATION FLOWCHART

amend names

OFFICERS RESPONSIBLE FOR THE RISK ASSESSMENT OF A CHIS

WHO CAN PROVIDE AUTHORISATION UNDER RIPA

CHIEF EXECUTIVE (LYNN AISBETT), STRATEGIC DIRECTORS (CHRISTINE MARSHALL, KEITH AUBREY)

HEAD OF COMMUNITIES
&
HEAD OF REGULATORY SERVICES

IF:

- **IT IS LIKELY THAT CONFIDENTIAL INFORMATION WILL BE GAINED OR**
- **THE INVESTIGATION IS NOT UNDER A REGULATORY FUNCTION EG A CONTRACTOR, EMPLOYEE OR**
- **A VULNERABLE PERSON IS TO BE USED AS A SOURCE THEN ONLY THE CHIEF EXECUTIVE CAN AUTHORISE**

RISK ASSESSOR

HEADS OF SERVICE (DIFFERENT FROM AUTHORISING OFFICER)

MANAGER OF CHIS

ANGELA TEBBUTT – HEAD OF COMMUNICATIONS

HARRINDER RAI – HEAD OF COMMUNITIES

DAWN GARTON – HEAD OF CENTRAL SERVICES

JIM WORLEY – HEAD OF REGULATORY SERVICES

HANDLER OF CHIS

INVESTIGATING OFFICERS

FOR ALL OTHER AUTHORISATIONS SEE THE DIRECTORS

SITE:	Melton B.C	**TASK BEING ASSESSED**	DATE:	00-00-2003
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											
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

APPENDIX 2 – Blank forms

RIPA PART II

- **Application for authorisation to carry out directed surveillance**
- **Application for renewal of authorisation for directed surveillance**
- **Review of directed surveillance authorisation**
- **Cancellation of directed surveillance authorisation**
- **Application for authorisation of the use or conduct of a CHIS**
- **Application for renewal of the use or conduct of a CHIS**
- **Review of a CHIS authorisation**
- **Cancellation of the use or conduct of a CHIS**
- **Record of oral authorisation for directed surveillance or use of or conduct of a CHIS**

RIPA PART I CHAPTER II

- **Application for authorisation to obtain disclosure of communications data**
- **Notice to request disclosure of communication data.**
- **SPOC officer report**
- **SPOC officer log sheet**

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

Unique Reference Number	

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Unique Reference Number	

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

<u>Describe precautions you will take to minimise collateral intrusion.</u>

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?

10. Confidential information [Code paragraphs 4.1 to 4.31].

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Unique Reference Number	

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

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

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

Unique Reference Number	

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3]. Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

Date of first review	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		Grade / Rank		
Signature		Date and time		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]				

Unique Reference Number	

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		

Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

Unique Reference Number	

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.

Unique Reference Number	

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

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

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

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

7. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

Unique Reference Number	

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

9. Authorising Officer's Statement.			
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (Print)	.....	**Grade / Rank**	- - - - - - - - - - - - - - - - - -
Signature	- - - - - - - - - - - - - - - - - -	**Date**	- - - - - - - - - - - - - - - - - - - -
Renewal From:	**Time:**	**Date:**	

Date of first review.	
Date of subsequent reviews of this authorisation.	

Unique Reference Number	

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.

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

Unique Reference Number	

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

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

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

7. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].

Unique Reference Number	

Name (Print)	.....	**Grade / Rank**	- - - - - - - - - - - - - - - - - - - -
Signature	- - - - - - - - - - - - - - - - -	**Date**	- - - - - - - - - - - - - - - - - - - -

10. Date of next review.	

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Public Authority *(including full address)*	

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

Details of cancellation:

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

Unique Reference Number	

2. Explain the value of surveillance in the operation:

3. Authorising officer's statement.			
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	.....	**Grade**	.....
Signature	.....	**Date**	.....

4. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled.	Date:	Time:

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

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

Application for authorisation of the 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)			

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [2] *Where appropriate throughout amend references to the Order relevant to your authority.*
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail <u>the purpose</u> for which the source will be tasked or used.
4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.

[2] For local authorities: The formal position of the authorising officer should be given. For example, Head of Trading Standards.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

5. Identify on which grounds the conduct or the use of the source is <u>necessary</u> under Section 29(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (eg. SI 2010 No.521).*

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

6. Explain <u>why</u> this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 3.2].

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

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

8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source (see Code paragraphs 3.17 to 3.18)?

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.14).
10. Explain <u>why</u> this conduct or use of the source is proportionate to what it seeks to achieve. **How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means [Code paragraphs 3.3 to 3.5]?**
11. Confidential information [Code paragraphs 4.1 to 4.21] **Indicate the likelihood of acquiring any confidential information.**
References for any other linked authorisations:
12. Applicant's Details.

Name (print)		**Grade/Rank/Position**	
Signature		**Tel No:**	
Date			

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

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

14. Explain <u>why</u> you believe the conduct or use of the source is necessary [Code paragraph 3.2]
Explain <u>why</u> you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement [Code paragraphs 3.3 to 3.5].

15. Confidential Information Authorisation. Supply details demonstrating compliance with Code paragraphs 4.1 to 4.21

16. Date of first review:	

17. Programme for subsequent reviews of this authorisation [Code paragraphs 5.15 and 5.16]. Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

18. Authorising Officer's Details			
Name (Print)		**Grade/Rank/Position**	
Signature		Time and date granted* Time and date authorisation ends	

**** Remember, an authorisation must be granted for a 12 month period, i.e. 1700 hrs 4th June 2006 to 2359hrs 3 June 2007***

19. Urgent Authorisation [Code paragraphs 5.13 and 5.14]: Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.
20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer

21. Authorising Officer of urgent authorisation				
Name (Print)		**Grade/Rank/Position**		
Signature		**Date and Time**		
Urgent authorisation expiry date:		**Expiry time:**		
Remember the 72 hour rule for urgent authorisations – check Code of Practice [Code Paragraph 5.14]. e.g. authorisation granted at 1700 on 1st June 2006 expires 1659 on 4th June 2006				

Unique Operation Reference Number* (*Filing Ref)	

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

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

(Please attach the original authorisation)

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**

Unique Operation Reference Number* (*Filing Ref)	

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

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

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

5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.

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

Unique Operation Reference Number* (*Filing Ref)	

7. Detail the results of regular reviews of the use of the source.

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

9. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

10.Authorising Officer's Comments. <u>This box must be completed.</u>

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

Unique Operation Reference Number* (*Filing Ref)	

Name (Print)	.....	**Grade / Rank**
Signature		**Date**
Renewal From:	**Time:**	**Date:** **End date/time of the authorisation**

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

Date of first review:	
Date of subsequent reviews of this authorisation:	

Unique Operation Reference Number* (*Filing Ref)	

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

Review of a Covert Human Intelligence Source (CHIS) Authorisation

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	

Unique Operation Reference Number* (*Filing Ref)	

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 information has been obtained and the value of the information so far obtained.

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

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

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

Unique Operation Reference Number* (*Filing Ref)	

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

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

8. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

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

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.			
Name (Print)	.....	Grade / Rank	
Signature	.....	Date	

Date of next review:	

Unique Operation Reference Number* (*Filing Ref)	

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

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

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)			

Unique Operation Reference Number* (*Filing Ref)	

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:
2. Explain the value of the source in the operation:

3. Authorising officer's statement. THIS SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.			
Name (Print)	.....	**Grade**	.....
Signature	.....	**Date**	.....

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

MELTON BOROUGH COUNCIL

RECORD OF ORAL AUTHORISATION FOR DIRECTED SURVEILLANCE OR USE OF COVERT HUMAN INTELLIGENCE SOURCE
(to be completed by the authorising officer)

Under the Regulation of Investigatory Powers Act 2000 limited to 72 hours only

1. NAME OF FILE

2. APPLICANT OFFICER

3. LOCATION

4. SUBJECTS

Name/Description and Address:

5. OFFENCE OR MATTER UNDER INVESTIGATION

Planning	☐	Health and Safety	☐
Licensing	☐	Antisocial Behaviour	☐
Housing Benefit	☐	Food Safety	☐
Council Tax	☐	Noise Nuisance	☐
Environmental Protection	☐	Other Please Specify	☐

☐

6. DETAILS AND OBJECTIVES OF THE SURVEILLANCE OR CHIS

7. NECESSITY OF SURVEILLANCE OR CHIS

8. PROPORTIONALITY OF SURVEILLANCE OR COVERT HUMAN INTELLIGENCE

9. REASONS FOR URGENCY

10. DATE AND TIME ORAL AUTHORISATION GIVEN

11. NAME OF AUTHORISING OFFICER: .....

Position: .....

Telephone Number: .....

SIGNATURE .....

MELTON BOROUGH COUNCIL

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**	
15) ASSESSMENT BY ACCREDITED SPoC.			
How much will the acquisition of the data cost?			
Are there other factors the DP should be aware of? *For example, the requirement:* • *is NOT reasonably practical for the CSP to do;* • *will cause an adverse cost or resource implication to either your public authority or the CSP (for instance does the investigation or operation have the analytical capacity to undertake analysis of the communications data once acquired);* • *will produce excess data to that required.*			
Name of Accredited SPoC			

16) AUTHORISATION (Completed by Accredited SPoC when appropriate)

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

☐ There is an agreement in place between the public authority and the CSP relating to the appropriate mechanisms for the disclosure of the data ◇

☐ The designated person considers there is a requirement to identify to whom a service is provided (for example subscriber check) but a CSP has yet to be conclusively determined as the holder of the communications data ♦

☐ CSP is not capable of obtaining or disclosing the communications data Δ

Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought. **Describe the course of conduct required to obtain the data.**	☐ ◇Traffic or Service Use data – acquisition by SPoC directly from CSP ☐ ♦ Subscriber Information – acquisition by SPoC or, where SPoC can not acquire data directly from CSP, serve assurance of the Authorisation on CSP[3] ☐ ΔOther conduct – specify

The statutory purpose for which the conduct may be authorised is set out at section 8 of this form.

The office, rank or position of the designated person should be recorded within section 17 of this form together with a record of the date & time the granting of an authorisation is made.

17. DESIGNATED PERSON

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

- *Why do you **believe** acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act;*
- *Why do you **believe** the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgement you should take in consideration any additional information from the SPoC. If the applicant has identified any meaningful degree of collateral intrusion, why you **believe** the request remains justified and proportionate to the objective(s)?*

My considerations in approving / not approving this application are:

☐ I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form. ☐ I give Notice and require the SPoC to serve it on (insert name of CSP) . The Notice bears the unique reference number			
Name		**Office, Rank or Position**	
Signature		**Time and Date**	

[1] See paragraph 3.30 of the code

MELTON BOROUGH COUNCIL

NOTICE

Section 22(4) of the Regulation of Investigatory Powers Act 2000

Where it appears to the designated person that a CSP is or may be in possession of, or be capable of obtaining, any communications data, the designated person 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[4] 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**			

[4] 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@homeoffice.gsi.gov.uk

MELTON BOROUGH 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**	

MELTON BOROUGH 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**

APPENDIX 3 – Home Office Code of Practice for the use of Directed Surveillance Amended to conform with SI 2003 3171

The Codes of practice are reproduced below. Following each code is a hyper link to the Home Office web site where they can be found along with further Home Office advice. The Authorisation forms can be found on this site at 'What's new'. These forms have been updated to include the latest amendments.

[NOTE: MELTON B. C. IS ONLY AUTHORISED FOR THE USE OF DIRECTED SURVEILLANCE OR CONDUCT AND USE OF A COVERT HUMAN INTELLIGENCE SOURCE. AUTHORISING OFFICERS ARE THE CHIEF OFFICERS]

COVERT SURVEILLANCE
CODE OF PRACTICE
Pursuant to Section 71 of the
Regulation of Investigatory Powers Act 2000
Commencement

This code applies to every authorisation of covert surveillance or of entry on or interference with property or with wireless telegraphy carried out under section 5 of the Intelligence Services Act 1994, Part III of the Police Act 1997 or Part II of the Regulation of Investigatory Powers Act 2000 by public authorities which begins on or after the day on which this code comes into effect.

CONTENTS

1.1 In this code the:

- **"1989 Act"** means the Security Service Act 1989;
- **"1994 Act"** means the Intelligence Services Act 1994;
- **"1997 Act"** means the Police Act 1997;
- **"2000 Act"** means the Regulation of Investigatory Powers Act 2000;
- **"RIP(S)A"** means the Regulation of Investigatory Powers (Scotland) Act 2000.

1.2 This code of practice provides guidance on the use of covert surveillance by public authorities under Part II of the 2000 Act and on entry on, or interference with, property (or with wireless telegraphy) under section 5 of the 1994 Act or Part III of the 1997 Act. This code replaces the code of practice issued in 1999 pursuant to section 101(3) of the 1997 Act.

1.3 General observation forms part of the duties of many law enforcement officers and other public authorities and is not usually regulated by the 2000 Act. For example, police officers will be on patrol to prevent and detect crime, maintain public safety and prevent disorder or trading standards or HM Customs and Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

1.4 Although, the provisions of the 2000 Act or of this code of practice do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use covert CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for intrusive or directed surveillance may be necessary.

1.5 The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of the code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers 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.

General extent of powers

1.6 Authorisations under the 2000 Act can be given for surveillance both inside and outside the United Kingdom. Authorisations for actions outside the United Kingdom can only validate them for the purposes of proceedings in the United Kingdom. An authorisation under Part II of the 2000 Act does not

take into account the requirements of the country outside the United Kingdom in which the investigation or operation is taking place.

1.7 Where the conduct authorised is likely to take place in Scotland, authorisations should be granted under RIP(S)A, unless the authorisation is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000; SI No. 2418). Additionally any authorisation granted or renewed for the purposes of national security or the economic well-being of the United Kingdom must be made under the 2000 Act. This code of practice is extended to Scotland in relation to authorisations made under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to authorisations made under RIP(S)A.

Use of material in evidence

1.8 Material obtained through covert surveillance may be used as evidence in criminal proceedings. The proper authorisation of surveillance should ensure the admissibility of such evidence under the common law, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998. Furthermore, the product of the surveillance described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996, where those rules apply to the law enforcement body in question.

Directed surveillance, intrusive surveillance and entry on or interference with property or with wireless telegraphy.

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

- **a. for the purposes of a specific investigation or 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 specifically identified for the purposes of the investigation or operation); and**
- **c. otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought for the carrying out of the surveillance.**

1.10 Directed surveillance investigations or operations can only be carried out by those public authorities who are listed in or added to Part I and Part II of schedule 1 of the 2000 Act.

1.11 intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

- **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.**

1.12 Applications to carry out intrusive surveillance can only be made by the senior authorising officer of those public authorities listed in or added to section 32(6) of the 2000 Act or by a member or official of those public authorities listed in or added to section 41(1).

1.13 Applications to enter on or interfere with property or with wireless telegraphy can only be made by the authorising officers of those public authorities listed in or added to section 93(5) of the 1997 Act. Under section 5 of the 1994 Act only members of the intelligence services are able to make applications to enter on or interfere with property or with wireless telegraphy.

GENERAL RULES ON AUTHORISATIONS

2.1 An authorisation under Part II of the 2000 Act will provide lawful authority for a public authority to carry out surveillance. Responsibility for authorising surveillance investigations or operations will vary, depending on whether the authorisation is for intrusive surveillance or directed surveillance, and which public authority is involved. For the purposes of Chapter 2 and 3 of this code the authorising officer, senior authorising officer or the person who makes an application to the Secretary of State will be referred to as an 'authorising officer'.

2.2 Part II of the 2000 Act does not impose a requirement on public authorities to seek or obtain an authorisation where, under the 2000 Act, one is available (see section 80 of the 2000 Act). Nevertheless, where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

2.3 Public authorities are therefore strongly recommended to seek an authorisation where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

Necessity and Proportionality

2.4 Obtaining an authorisation under the 2000 Act, the 1997 Act and 1994 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. The 2000 Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 28(3) of the 2000 Act for directed surveillance and in section 32(3) of the 2000 Act for intrusive surveillance.

2.5 Then, 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 the objective in question and must not be arbitrary or unfair.

Collateral Intrusion

2.6 Before authorising surveillance the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

2.7 An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the surveillance.

2.8 Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and reauthorised or a new authorisation is required.

2.9 Any person granting or applying for an authorisation or warrant will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. In this regard, it is recommended that where the authorising officers in the National Criminal Intelligence Service (NCIS), the National Crime Squad (NCS) and HM Customs and Excise (HMCE) consider that conflicts might arise they should consult a senior officer within the police force area in which the investigation or operation takes place.

2.10 The matters in paragraphs 2.1 – 2.9 above must also be taken into account when applying for authorisations or warrants for entry on or interference with property or with wireless telegraphy. In particular they must be necessary in the circumstances of the particular case for one of the statutory ground listed in section 93(2)(a) of the 1997 Act and section 5(2)(c) of the 1994 Act, proportionate and when exercised steps should be taken to minimise collateral intrusion.

Combined authorisations

2.11 A single authorisation may combine:

- two or more different authorisations under Part II of the 2000 Act;
- an authorisation under Part II of the 2000 Act and an authorisation under Part III of the 1997 Act;
- a warrant for intrusive surveillance under Part II of the 2000 Act and a warrant under section 5 of the 1994 Act.

2.12 For example, a single authorisation may combine authorisations for directed and intrusive surveillance. The provisions applicable in the case of each of the authorisations must be considered separately. Thus, a police superintendent can authorise the directed surveillance but the intrusive surveillance needs the separate authorisation of a chief constable, and in certain cases the approval of a Surveillance Commissioner will also be necessary. Where an authorisation for directed surveillance or the use or conduct of a covert human intelligence source is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State. However, this does not preclude public authorities from obtaining separate authorisations.

2.13 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by the Armed Forces on behalf of the police, authorisations would be sought by the police and granted by the appropriate authorising officer. In cases where the Security Service is acting in support of the police or other law enforcement agencies in the field of serious crime, the Security Service would normally seek authorisations.

Central Record of all authorisations

2.14 A centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for a period of at least three years from the ending of the authorisation and should contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why.
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorisation was cancelled.

2.15 In all cases, the relevant authority should maintain the following documentation which need not form part of the centrally retrievable record:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the authorising officer.

Retention and destruction of the product

2.16 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

2.17 In the cases of the law enforcement agencies (not including the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

2.18 There is nothing in the 2000 Act which prevents material obtained from properly authorised surveillance from being used in other investigations. Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

The Intelligence Services, MOD and HM Forces

2.19 The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

3 SPECIAL RULES ON AUTHORISATIONS

3.1 The 2000 Act does not provide any special protection for 'confidential information'. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. So, for example, extra care should be given where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.
3.2 In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. Annex A lists the authorising officer for each public authority permitted to authorise such surveillance.

Communications Subject to Legal Privilege

3.3 Section 98 of the 1997 Act describes those matters that are subject to legal privilege in England and Wales. In Scotland, the relevant description is contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.
3.4 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.
3.5 The 2000 Act does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and surveillance which acquires such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8. Legally privileged information obtained by surveillance is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, the mere fact that such surveillance has taken place may lead to any related criminal proceedings being stayed as an abuse of process. Accordingly, action which may lead to such information being acquired is subject to additional safeguards under this code.
3.6 In general, an application for surveillance which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances. Full regard should be had to the particular proportionality issues such surveillance raises. The application should include, in addition to the reasons why it is considered necessary for the surveillance to take place, an assessment of how likely it is that information subject to legal privilege will be acquired. In addition, the application should clearly state whether the purpose (or one of the purposes) of the surveillance is to obtain legally privileged information.
3.7 This assessment will be taken into account by the authorising officer in deciding whether the proposed surveillance is necessary and proportionate under section 28 of the 2000 Act for directed surveillance and under section 32 for intrusive surveillance. The authorising officer may require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where legally privileged information has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.
3.8 A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, any case where a lawyer is the subject of an investigation or operation should be notified to the relevant Commissioner during his next inspection and any material which has been retained should be made available to him if requested.
3.9 Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information. Any dissemination

of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Communications involving Confidential Personal Information and Confidential Journalistic Material

3.10 Similar consideration must also be given to authorisations that involve confidential personal information and confidential journalistic material. In those cases where confidential personal information and confidential journalistic material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

3.11 Spiritual counselling means conversations between an individual and a Minister of Religion acting in his official capacity, where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

3.12 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.

4 AUTHORISATION PROCEDURES FOR DIRECTED SURVEILLANCE

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

d. for the purposes of a specific investigation or specific operation;
e. in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
f. otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought for the carrying out of the surveillance.

4.2 Covert surveillance is defined in section 26(9)(a) of the 2000 Act as any 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.

4.3 Private information is defined in section 26(10) of the 2000 Act as including any information relating to a person's private or family life. The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. Family life should be treated as extending beyond the formal relationships created by marriage.

4.4 Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

4.5 By virtue of section 48(4) of the 2000 Act, surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication (as the case may be). For further details see paragraphs 4.30 - 4.32 of this code.

4.6 Surveillance in residential premises or in private vehicles is defined as intrusive surveillance in section 26(3) of the 2000 Act and is dealt with in chapter 5 of this code. However, where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance and should be authorised accordingly.

4.7 Directed surveillance does not include entry on or interference with property or with wireless telegraphy. These activities are subject to a separate regime of authorisation or warrantry, as set out in chapter 6 of this code.

4.8 Directed surveillance includes covert surveillance within office premises, (as defined in paragraph 6.31 of this code). Authorising officers are reminded that confidential information should be afforded an enhanced level of protection. Chapter 3 of this code provides that in cases where the likely consequence of surveillance is to acquire confidential information, the authorisation should be given at a higher level.

Authorisation Procedures

4.9 Under section 28(3) of the 2000 Act an authorisation for directed surveillance may be granted by an authorising officer where he believes that the authorisation is necessary in the circumstances of the particular case:

- in the interests of national security[1],[2] ;
- for the purpose of preventing and detecting [3] crime or of preventing disorder;
- in the interests of the economic well-being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health[4];
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for any other purpose prescribed by an order made by the Secretary of State.[5]

4.10 The authorising officer must also believe that the surveillance is proportionate to what it seeks to achieve.

4.11 The public authorities entitled to authorise directed surveillance are listed in Schedule 1 to the 2000 Act. Responsibility for authorising the carrying out of directed surveillance rests with the authorising officer and requires the personal authority of the authorising officer. The Regulation of Investigatory Powers (Prescriptions of Offices, Ranks and Positions) Order 2003; SI No: 3171 designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases. Where an authorisation for directed surveillance is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State.

4.12 The authorising officer must give authorisations in writing, except that in urgent cases, they may be given orally by the authorising officer or the officer entitled to act in urgent cases. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant as soon as is reasonably practicable.

4.13 A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making.

4.14 Authorising officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently. Where an authorising officer authorises such an investigation or operation the central record of authorisations (see paragraphs 2.14 -2.15) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

4.15 Authorising officers within the Police, NCIS and NCS may only grant authorisations on application by a member of their own force, Service or Squad. Authorising officers in HMCE may only grant an authorisation on application by a customs officer.[6]

Information to be provided in applications for authorisation

4.16 A written application for authorisation for directed surveillance should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

4.17 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given; and/or
- the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

4.18 Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

Duration of authorisations

4.19 A written authorisation granted by an authorising officer will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect.

4.20 Urgent oral authorisations or written authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation was granted or renewed.

Reviews

4.21 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations (see paragraphs 2.14 - 2.15). Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

4.22 In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Renewals

4.23 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of three months unless it is a case to which paragraph 4.25 applies. Renewals may also be granted orally in urgent cases and last for a period of seventy-two hours.

4.24 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

4.25 If at any time before an authorisation for directed surveillance, granted on the grounds of it being in the interests of national security or in the interests of the economic well-being of the UK, would cease to have effect, an authorising officer who is a member of the intelligence services considers it necessary for it to continue, he may renew it for a further period of **six months**, beginning with the day on which it would have ceased to have effect but for the renewal.

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

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in paragraph 4.16;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

4.27 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations (see paragraphs 2.14 - 2.15).

Cancellations

4.28 The authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794).

Ceasing of surveillance activity

4.29 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction

was given should be recorded in the central record of authorisations (see paragraphs 2.14 - 2.15) and the notification of cancellation where relevant

ADDITIONAL RULES

Recording of telephone conversations

4.30 Subject to paragraph 4.31 below, the interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be authorised only by the Secretary of State, in accordance with the terms of Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.

4.31 Part I of the 2000 Act provides certain exceptions to the rule that interception of telephone conversations must be warranted under that Part. This includes, where one party to the communication consents to the interception, it may be authorised in accordance with section 48(4) of the 2000 Act provided that there is no interception warrant authorising the interception. In such cases, the interception is treated as directed surveillance.

4.32 The use of a surveillance device should not be ruled out simply because it may incidentally pick up one or both ends of a telephone conversation, and any such product can be treated as having been lawfully obtained. However, its use would not be appropriate where the sole purpose is to overhear speech which, at the time of monitoring, is being transmitted by a telecommunications system. In such cases an application should be made for an interception of communication warrant under section 5 of the 2000 Act.

5 AUTHORISATION PROCEDURES FOR INTRUSIVE SURVEILLANCE

5.1 Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

g. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

h. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

5.2 Covert surveillance is defined in section 26(9)(a) of the 2000 Act as any 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.

5.3 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.

5.4 Residential premises are defined in section 48(1) of the 2000 Act. The definition includes hotel rooms, bedrooms in barracks, and police and prison cells but not any common area to which a person is allowed access in connection with his occupation of such accommodation e.g. a hotel lounge.

5.5 A private vehicle is defined in section 48(1) of the 2000 Act as any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it. A person does not have a right to use a motor vehicle if his right to use it derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey.

5.6 In many cases, a surveillance investigation or operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. In such cases, both activities need authorisation. This can be done as a combined authorisation (see paragraph 2.11).

5.7 An authorisation for intrusive surveillance may be issued by the Secretary of State (for the intelligence services, the Ministry of Defence, HM Forces and any other public authority designated under section 41(1)) or by a senior authorising officer (for police, NCIS, NCS and HMCE).

5.8 All authorisations require the personal authority of the Secretary of State or the senior authorising officer. Any members or officials of the intelligence services, the Ministry of Defence and HM Forces can apply to the Secretary of State for an intrusive surveillance warrant. Under section 32(2) of the 2000 Act neither the Secretary of State or the senior authorising officer may authorise intrusive surveillance unless he believes -

c. that the authorisation is necessary in the circumstances of the particular case on the grounds that it is:

- in the interests of national security;[7]
- for the purpose of preventing or detecting serious crime; or
- in the interests of the economic well-being of the UK;

and

b. the authorising officer must also believe that the surveillance is proportionate to what it seeks to achieve.

5.9 A factor which must be taken into account in deciding whether an authorisation is necessary and proportionate is whether the information which it is thought necessary to obtain by means of the intrusive surveillance could reasonably be obtained by other less intrusive means.

Authorisations Procedures for Police, National Criminal Intelligence Service, the National Crime Squad and HM Customs and Excise

5.10 The senior authorising officer should generally give authorisations in writing. However, in urgent cases, they may be given orally. In an urgent oral case, a statement that the senior authorising officer has expressly authorised the conduct should be recorded in writing by the applicant as soon as is reasonably practicable.

5.11 If the senior authorising officer is absent then as provided for in section 12(4) of the Police Act 1996, section 5(4) of the Police (Scotland) Act 1967, section 25 of the City of London Police Act 1839, or sections 8 or 54 of the 1997 Act, an authorisation can be given in writing or, in urgent cases, orally by the designated deputy.

5.12 In an urgent case, where it is not reasonably practicable having regard to the urgency of the case for the designated deputy to consider the application, a written authorisation may be granted by a person entitled to act under section 34(4) of the 2000 Act.

5.13 A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making.

5.14 The consideration of an authorisation by the senior authorising officer is only to be regarded as not reasonably practicable (within the meaning of section 34(2) of the 2000 Act) if he is on annual leave, is absent from his office and his home, or is for some reason not able within a reasonable time to obtain access to a secure telephone or fax machine. Pressure of work is not normally to be regarded as rendering it impracticable for a senior authorising officer to consider an application. Where a designated deputy gives an authorisation this should be made clear and the reason for the absence of the senior authorising officer given.

5.15 A police, NCIS or NCS authorisation cannot be granted unless the application is made by a member of the same force, service or squad. For HMCE an authorisation cannot be granted unless the application is made by a customs officer. Where the surveillance is carried out in relation to any residential premises, the authorisation cannot be granted unless the residential premises are in the area of operation of the force, service, squad or organisation.

Footnotes:

[7] A senior authorising officer of a law enforcement agency should not issue an authorisation for intrusive surveillance or entry on or interference with property or with wireless telegraphy where the operation is within the responsibilities of one of the intelligence services and properly falls to be authorised by warrant issued by the Secretary of State under Part II of the 2000 Act or the 1994 Act. Also see footnotes 1 and 2.

Information to be provided in applications for authorisation

5.16 Applications should be in writing and describe the conduct to be authorised and the purpose of the investigation or operation. The application should specify:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting serious crime) listed in section 32(3) of the 2000 Act;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the residential premises or private vehicle in relation to which the surveillance will take place;
- the identities, where known, of those to be the subject of the surveillance;

- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why the intrusion is justified;
- details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- A subsequent record should be made of whether authority was given or refused, by whom and the time and date.

5.17 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or designated deputy considered the case so urgent that an oral instead of a written authorisation was given; and/or
- the reasons why it was not reasonably practicable for the application to be considered by the senior authorising officer or the designated deputy.

5.18 Where the application is oral, the detail referred to above should be recorded in writing as soon as reasonably practicable.

Approval of Surveillance Commissioners

5.19 Except in urgent cases a police, NCIS, NCS or HMCE authorisation granted for intrusive surveillance will not take effect until it has been approved by a Surveillance Commissioner and written notice of the Commissioner's decision has been given to the person who granted the authorisation. This means that the approval will not take effect until the notice has been received in the office of the person who granted the authorisation within the relevant force, service, squad or HMCE.

5.20 When the authorisation is urgent it will take effect from the time it is granted provided notice is given to the Surveillance Commissioner in accordance with section 35(3)(b) (see section 36(3) of the 2000 Act).

5.21 There may be cases that become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the authorising officer should notify the Surveillance Commissioner that the case is now urgent (pointing out that it has become urgent since the notification). In these cases, the authorisation will take effect immediately.

Notifications to Surveillance Commissioners

5.22 Where a person grants, renews or cancels an authorisation, he must, as soon as is reasonably practicable, give notice in writing to a Surveillance Commissioner, in accordance with whatever arrangements have been made by the Chief Surveillance Commissioner.

5.23 In urgent cases, the notification must specify the grounds on which the case is believed to be one of urgency. The urgency provisions should not be used routinely. If the Surveillance Commissioner is satisfied that there were no grounds for believing the case to be one of urgency, he has the power to quash the authorisation

5.24 The information to be included in the notification to the Surveillance Commissioner is set out in the Regulation of Investigatory Powers (Notification of Authorisations etc.) Order 2000; SI No: 2563.

Authorisation Procedures for Secretary of State

5.25 An intrusive surveillance authorisation for any of the intelligence services, the Ministry of Defence, HM Forces or any other public authority designated for this purpose requires a Secretary of State authorisation/warrant, unless they are acting on behalf of another public authority that has obtained an authorisation. In this context, Secretary of State can mean any Secretary of State, although an authorisation or warrant should be obtained from the Secretary of State of the relevant department.

5.26 Intelligence services authorisations must be made by issue of a warrant. Such warrants will generally be given in writing by the Secretary of State. In urgent cases, a warrant may be signed (but not renewed) by a senior official, provided the Secretary of State has expressly authorised this.

5.27 Applications to the Secretary of State for authorisations should specify those matters listed in paragraph 5.16.

All intrusive surveillance authorisations

5.28 Paragraphs 5.29 to 5.42 deal with the duration, renewal and cancellation of authorisations. Unless otherwise specified the guidance below applies to all authorisations.

Duration of Authorisations

All authorisations except Secretary of State Intelligence Services authorisations

5.29 A written authorisation granted by a Secretary of State, a senior authorising officer or a designated deputy will cease to have effect (unless renewed) at the end of a period of **three months**, beginning with the day on which it took effect.

5.30 Oral authorisations given in urgent cases by a Secretary of State, a senior authorising officers or their designated deputies, and written authorisations given by those only entitled to act in urgent cases (see paragraph 5.11), will cease to have effect (unless renewed) at the end of the period of **seventy-two** hours beginning with the time when they took effect.

Secretary of State intelligence services authorisations

5.31 A warrant issued by the Secretary of State will cease to have effect at the end of a period of six months beginning with the day on which it was issued.

5.32 Warrants expressly authorised by a Secretary of State, and signed on his behalf by a senior civil servant, will cease to have effect at the end of the second working day following the day of issue of the warrant unless renewed by the Secretary of State.

Renewals

All authorisations except Secretary of State Intelligence Services authorisations

5.33 If at any time before an authorisation expires the senior authorising officer or, in his absence, the designated deputy considers the authorisation should continue to have effect for the purpose for which it was issued, he may renew it in writing for a further period of **three months**.

5.34 As with the initial authorisation, the senior authorising officer must (unless it is a case to which the urgency procedure applies) seek the approval of a Surveillance Commissioner. This means that the renewal will not take effect until the notice of it has been received in the office of the person who granted the authorisation within the relevant force, service, squad or HMCE (but not before the day on which the authorisation would have otherwise ceased to have effect). In urgent cases, a renewal can take effect immediately (provided this is not before the day on which the authorisation would have otherwise ceased to have effect). See section 35 and 36 of the 2000 Act and the Regulation of Investigatory Powers (Notification of Authorisations etc.) Order 2000; SI No: 2563.

5.35 Subject to paragraph 5.36, if at any time before the day on which a Secretary of State authorisation expires, the Secretary of State considers it necessary for the warrant to be renewed for the purpose for which it was issued, he may renew it in writing for a further period of three months, beginning with the day on which it would have ceased to have effect, but for the renewal.

Secretary of State intelligence services authorisations

5.36 If at any time before an intelligence service warrant expires, the Secretary of State considers it necessary for the warrant to be renewed for the purpose for which it was issued, he may renew it in writing for a further period of six months, beginning with the day on which it would have ceased to have effect, but for the renewal.

5.37 All applications for a renewal of an authorisation or warrant should record:

- whether this is the first renewal or every occasion on which the warrant/authorisation has been renewed previously;
- any significant changes to the information listed in paragraph 5.16;
- the reasons why it is necessary to continue with the intrusive surveillance;
- the content and value to the investigation or operation of the product so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

5.38 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations (see paragraphs 2.14 - 2.15).

Reviews

5.39 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations (see paragraphs 2.14 - 2.15). Particular attention is drawn to the need to review authorisations frequently where the intrusive surveillance provides access to confidential information or involves collateral intrusion.

5.40 The senior authorising officer or, for those subject to Secretary of State authorisation, the member or official who made the application within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Cancellations

5.41 The senior authorising officer who granted or last renewed the authorisation must cancel it, or the person who made the application to the Secretary of State must apply for its cancellation, if he is satisfied that the surveillance no longer meets the criteria upon which it was authorised. Where the senior authorising officer or

person who made the application to the Secretary of State is no longer available, this duty will fall on the person who has taken over the role of senior authorising officer or taken over from the person who made the application to the Secretary of State or the person who is acting as the senior authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794).

5.42 The Surveillance Commissioners must be notified where police, NCIS, NCS or HMCE authorisations are cancelled (see the Regulation of Investigatory Powers (Notification of Authorisations etc.) Order 2000; SI No: 2563).

Ceasing of surveillance activity

5.43 As soon as the decision is taken that the intrusive surveillance should be discontinued, instructions must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central record of authorisations (see paragraphs 2.14 - 2.15) and the notification of cancellation where relevant.

Police, National Criminal Intelligence Service, the National Crime Squad and HM Customs and Excise authorisations

5.44 In cases where an authorisation is quashed or cancelled by a Surveillance Commissioner, the senior authorising officer must immediately instruct those carrying out the surveillance to stop monitoring, observing, listening or recording the activities of the subject of the authorisation. The date and time when such an instruction was given should be recorded on the central record of authorisations (see paragraphs 2.14 - 2.15).

6 AUTHORISATION PROCEDURES FOR ENTRY ON OR INTERFERENCE WITH PROPERTY OR WITH WIRELESS TELEGRAPHY

6.1 The 1994 Act and 1997 Act provide lawful authority for entry on or interference with property or with wireless telegraphy by the intelligence services and the police, NCIS, NCS and HMCE.

6.2 In many cases a covert surveillance operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. This can be done as a combined authorisation, although the criteria for authorisation of each activity must be considered separately (see paragraph 2.11).

Authorisations for entry on or interference with property or with wireless telegraphy by the police, National Criminal Intelligence Service, the National Crime Squad and HM Customs and Excise

6.3 Responsibility for such authorisations rests with the authorising officer as defined in section 93(5) of the 1997 Act, that is the chief constable or equivalent. Authorisations require the personal authority of the authorising officer (or his designated deputy) except in urgent situations, where it is not reasonably practicable for the application to be considered by such person. The person entitled to act in such cases is set out in section 94 of the 1997 Act.

6.4 Authorisations under the 1997 Act may not be necessary where the public authority is acting with the consent of a person able to give permission in respect of relevant property, although consideration should still be given to the need to obtain an authorisation under Part II of the 2000 Act.

6.5 Authorisations for the police, NCIS and NCS may only be given by an authorising officer on application by a member of his own force, Service or Squad for entry on or interference with property or with wireless telegraphy within the authorising officer's own area of operation. For HMCE an authorisation may only be given by an authorising officer on application by a customs officer. An authorising officer may authorise the taking of action outside the relevant area solely for the purpose of maintaining or retrieving any device, apparatus or equipment.

6.6 Any person giving an authorisation for entry on or interference with property or with wireless telegraphy under section 93(2) of the 1997 Act must believe that:

- it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime (or in the case of the Police Service of Northern Ireland, in the interests of national security)[8]; and
- that the taking of the action is proportionate to what the action seeks to achieve.

6.7 The authorising officer must take into account whether what it is thought necessary to achieve by the authorised conduct could reasonably be achieved by other means.

6.8 Any person granting or applying for an authorisation or warrant to enter on or interfere with property or with wireless telegraphy will also need to be aware of particular sensitivities in the local community where the entry or interference is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment. In this regard, it is recommended that the authorising officers in NCIS, NCS

and HMCE should consult a senior officer within the police force in which the investigation or operation takes place where the authorising officer considers that conflicts might arise. The Chief Constable of the Police Service of Northern Ireland should be informed of any surveillance operation undertaken by another law enforcement agency which involve its officers in maintaining or retrieving equipment in Northern Ireland.

Authorisation procedures for entry on or interference with property or with wireless telegraphy by the police, National Criminal Intelligence Service, the National Crime Squad and HM Customs and Excise

6.9 Authorisations will generally be given in writing by the authorising officer. However, in urgent cases, they may be given orally by the authorising officer. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant as soon as is reasonably practicable. This should be done by the person with whom the authorising officer spoke.

6.10 If the authorising officer is absent then as provided for in section 12(4) of the Police Act 1996, section 5(4) of the Police (Scotland) Act 1967, section 25 of the City of London Police Act 1839, or sections 8 or 54 of the 1997 Act, an authorisation can be given in writing or, in urgent cases, orally by the designated deputy.

6.11 Where, however, in an urgent case, it is not reasonably practicable for the designated deputy to consider an application, then written authorisation may be given by the following:

- in the case of the police, by an assistant chief constable (other than a designated deputy);
- in the case of the Metropolitan Police and City of London Police, by a commander;
- in the case of NCIS and NCS, by a person designated by the relevant Director General[9];
- in the case of HMCE, by a person designated by the Commissioners of Customs and Excise[10.]

6.12 Applications to the authorising officer for authorisation must be made in writing by a police or customs officer or a member of NCIS or NCS (within the terms of section 93(3) of the 1997 Act) and should specify:

- the identity or identities of those to be targeted (where known);
- the property which the entry or interference with will affect;
- the identity of individuals and/or categories of people, where known, who are likely to be affected by collateral intrusion;
- details of the offence planned or committed;
- details of the intrusive surveillance involved;
- how the authorisation criteria (as set out in paragraphs 6.6 and 6.7) have been met;
- any action which may be necessary to retrieve any equipment used in the surveillance;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an authorisation was given or refused, by whom and the time and date.

6.13 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or designated deputy considered the case so urgent that an oral instead of a written authorisation was given; and
- the reasons why (if relevant) the person granting the authorisation did not consider it reasonably practicable for the application to be considered by the senior authorising officer or the designated deputy.

6.14 Where the application is oral, the information referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

Notifications to Surveillance Commissioners

6.15 Where a person gives, renews or cancels an authorisation, he must, as soon as is reasonably practicable, give notice of it in writing to a Surveillance Commissioner, in accordance with arrangements made by the Chief Surveillance Commissioner. In urgent cases which would otherwise have required the approval of a Surveillance Commissioner, the notification must specify the grounds on which the case is believed to be one of urgency.

6.16 There may be cases which become urgent after approval has been sought but before a response has been received from a Surveillance Commissioner. In such a case, the authorising officer should notify the Surveillance Commissioner that the case is urgent (pointing out that it has become urgent since the previous notification). In these cases, the authorisation will take effect immediately.

6.17 Notifications to Surveillance Commissioners in relation to the authorisation, renewal and cancellation of authorisations in respect of entry on or interference with property should be in accordance with the requirements of the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No. 3241.

Duration of authorisations

6.18 Written authorisations given by authorising officers will cease to have effect at the end of a period of three months beginning with the day on which they took effect. In cases requiring prior approval by a Surveillance Commissioner this means from the time the Surveillance Commissioner has approved the authorisation and the person who gave the authorisation has been notified. This means that the approval will not take effect until the notice has been received in the office of the person who granted the authorisation within the relevant force, service, squad or HMCE. In cases not requiring prior approval, this means from the time the authorisation was given.

6.19 Oral authorisations given in urgent cases by:

- authorising officers;
- or designated deputies

and written authorisations given by:

- assistant chief constables (other than a designated deputy);
- commanders in the Metropolitan Police and City of London Police;
- the person designated to act by the Director General of NCIS or of NCS;
- the person designated for the purpose by the Commissioners of Customs and Excise;

will cease at the end of the period of **seventy-two** hours beginning with the time when they took effect.

Renewals

6.20 If at any time before the day on which an authorisation expires the authorising officer or, in his absence, the designated deputy considers the authorisation should continue to have effect for the purpose for which it was issued, he may renew it in writing for a period of **three months** beginning with the day on which the authorisation would otherwise have ceased to have effect. Authorisations may be renewed more than once, if necessary, and the renewal should be recorded on the authorisation record (see paragraph 6.27).

6.21 Commissioners must be notified of renewals of authorisations. The information to be included in the notification is set out in the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No: 3241.

6.22 If, at the time of renewal, the criteria in paragraph 6.30 exist, then the approval of a Surveillance Commissioner must be sought before the renewal can take effect. The fact that the initial authorisation required the approval of a Commissioner before taking effect does not mean that its renewal will automatically require such approval. It will only do so if, at the time of the renewal, it falls into one of the categories requiring approval (and is not urgent).

Reviews

6.23 Authorising officers should regularly review authorisations to assess the need for the entry on or interference with property or with wireless telegraphy to continue. This should be recorded on the authorisation record (see paragraph 6.27). The authorising officer should determine how often a review should take place when giving an authorisation. This should be as frequently as is considered necessary and practicable and at no greater interval than one month. Particular attention is drawn to the need to review authorisations and renewals regularly and frequently where the entry on or interference with property or with wireless telegraphy provides access to confidential information or involves collateral intrusion.

Cancellations

6.24 The senior authorising officer who granted or last renewed the authorisation must cancel it, or the person who made the application to the Secretary of State must apply for its cancellation, if he is satisfied that the authorisation no longer meets the criteria upon which it was authorised. Where the senior authorising officer or person who made the application to the Secretary of State is no longer available, this duty will fall on the person who has taken over the role of senior authorising officer or taken over from the person who made the application to the Secretary of State or the person who is acting as the senior authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794).

6.25 The Surveillance Commissioners must be notified of cancellations of authorisations. The information to be included in the notification is set out in the Police Act 1997 (Notifications of Authorisations etc) Order 1998; SI No: 3421.

6.26 The Surveillance Commissioners have the power to cancel an authorisation if they are satisfied that, at any time after an authorisation was given or renewed, there were no reasonable grounds for believing the matters set out in paragraphs 6.6 and 6.7 above. In such circumstances, a Surveillance Commissioner may order the

destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

Authorisation record

6.27 An authorisation record should be created which records:

- the time and date when an authorisation is given;
- whether an authorisation is in written or oral form;
- the time and date when it was notified to a Surveillance Commissioner;
- and the time and date when the Surveillance Commissioner notified his approval (where appropriate).

The authorisation record should also record:

- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the authorisation;
- the date of every renewal; and
- it should record the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy.

Ceasing of entry on or interference with property or with wireless telegraphy

6.28 Once an authorisation or renewal expires or is cancelled or quashed, the authorising officer must immediately instruct those carrying out the surveillance to cease all the actions authorised for the entry on or interference with property or with wireless telegraphy. The time and date when such an instruction was given should be recorded on the authorisation record (see paragraph 6.27).

Retrieval of equipment

6.29 Where a Surveillance Commissioner quashes or cancels an authorisation or renewal, he will, if there are reasonable grounds for doing so, order that the authorisation remain effective for a specified period, to enable officers to retrieve anything left on the property by virtue of the authorisation. He can only do so if the authorisation or renewal makes provision for this. A decision by the Surveillance Commissioner not to give such an order can be the subject of an appeal to the Chief Surveillance Commissioner.

Footnotes:

[8]See footnotes 1 and 2.

[9]For police members of NCIS or NCS, this will be an officer who holds the rank of assistant chief constable in that Service or Squad. Additionally, in the case of NCIS, this may be an assistant chief investigation officer of HMCE.

[10]This will be an officer of the rank of assistant chief investigation officer.

Special Rules

Cases requiring prior approval of a Surveillance Commissioner

6.30 In certain cases, an authorisation for entry on or interference with property will not take effect until a Surveillance Commissioner has approved it and the notice has been received in the office of the person who granted the authorisation within the relevant force, service, squad or HMCE (unless the urgency procedures are used). These are cases where the person giving the authorisation believes that:

- any of the property specified in the authorisation:
- is used wholly or mainly as a dwelling or as a bedroom in a hotel; or
- constitutes office premises; or
- the action authorised is likely to result in any person acquiring knowledge of:
- matters subject to legal privilege;
- confidential personal information; or
- confidential journalistic material.

6.31 Office premises are defined as any building or part of a building whose sole or principal use is as an office or for office purposes (which means purposes of administration, clerical work, handling money and telephone or telegraph operation).

Authorisations for entry on or interference with property or with wireless telegraphy by the intelligence services

6.32 Before granting a warrant, the Secretary of State must:

- think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;
- be satisfied that the taking of the action is proportionate to what the action seeks to achieve;
- take into account in deciding whether an authorisation is necessary and proportionate is whether the information which it is thought necessary to obtain by the conduct authorised by the warrant could reasonably be obtained by other means; and
- be satisfied that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of disclosure of any material
- obtained by means of the warrant, and that material obtained will be subject to those arrangements.

6.33 An application for a warrant must be made by a member of the intelligence services for the taking of action in relation to that agency. In addition, the Security Service may make an application for a warrant to act on behalf of the Secret Intelligence Service (SIS) and the Governments Communication Headquarters (GCHQ). SIS and GCHQ may not be granted a warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

6.34 A warrant shall, unless renewed, cease to have effect if the warrant was under the hand of the Secretary of State, at the end of the period of **six months** beginning with the day on which it was issued. In any other case, at the end of the period ending with the **second working day** following that day.

6.35 If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of **six months** beginning with that day. The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary.

6.36 The intelligence services should provide the same information as the police, as and where appropriate, when making applications, requests for renewal and requests for cancellation of property warrants.

Retrieval of equipment

6.37 Because of the time it can take to remove equipment from a person's property it may also be necessary to renew a property warrant in order to complete the retrieval. Applications to the Secretary of State for renewal should state why it is being or has been closed down, why it has not been possible to remove the equipment and any timescales for removal, where known.

7 OVERSIGHT BY COMMISSIONERS

7.1 The 1997 and 2000 Acts require the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police and the Ministry of Defence Police and the British Transport Police), NCIS, the NCS, HMCE and of the 2000 Act the other public authorities listed in Schedule 1 and in Northern Ireland officials of the Ministry of Defence and HM Forces.

7.2 The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within Part II of the 2000 Act and the 1994 Act by the Security Service, Secret Intelligence Service, GCHQ and the Ministry of Defence and HM Forces (excluding the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police, and in Northern Ireland officials of the Ministry of Defence and HM Forces);

7.3 This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

7.4 References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other members of staff to whom such functions have been delegated.

8 COMPLAINTS

8.1 The 2000 Act establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ
020 7273 4514

Covert Surveillance Code of Practice

http://www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codeofpractice/surveillance/index.html

APPENDIX 4 – Home Office Code of Practice for the use or conduct of a Covert Human Intelligence Source Amended to conform with SI 2003 3171

COVERT HUMAN INTELLIGENCE SOURCES
CODE OF PRACTICE
Pursuant to Section 71 of the
Regulation of Investigatory Powers Act 2000
Commencement

This code applies to every authorisation of the use or conduct by public authorities of covert human intelligence sources carried out under Part II of the Regulation of Investigatory Powers Act 2000 which begins on or after the day on which this code comes into effect.

Chapter 1: BACKGROUND

1 GENERAL

1.1 In this code the:

- **"1989 Act"** means the Security Service Act 1989;
- **"1994 Act"** means the Intelligence Services Act 1994;
- **"1997 Act"** means the Police Act 1997;
- **"2000 Act"** means the Regulation of Investigatory Powers Act 2000;
- **"RIP(S)A"** means the Regulation of Investigatory Powers (Scotland) Act 2000;

1.2 This code of practice provides guidance on the authorisation of the use or conduct of covert human intelligence sources ("a source") by public authorities under Part II of the 2000 Act.

1.3 The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

1.4 Neither Part II of the 2000 Act or this code of practice is intended to affect the practices and procedures surrounding criminal participation of sources.

1.5 The 2000 Act provides that all codes of practice relating to the 2000 Act are admissible as evidence in criminal and civil proceedings. If any provision of the code appears relevant to any court or tribunal considering any such proceedings, or to the Investigatory Powers 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.

General extent of powers

1.6 Authorisations can be given for the use or conduct of a source both inside and outside the United Kingdom. Authorisations for actions outside the United Kingdom can only validate them for the purposes of proceedings in the United Kingdom. An authorisation under Part II of the 2000 Act does not take into account the requirements of the country outside the United Kingdom in which the investigation or operation is taking place.

1.7 Members of foreign law enforcement or other agencies or sources of those agencies may be authorised under the 2000 Act in the UK in support of domestic and international investigations.

1.8 Where the conduct authorised is likely to take place in Scotland, authorisations should be granted under RIP(S)A, unless the authorisation is being obtained by those public authorities listed in section 46(3) of the 2000 Act and the Regulation of Investigatory Powers (Authorisations Extending to Scotland) Order 2000). Additionally, any authorisation granted or renewed for the purposes of national security or the economic well-being of the UK must be made under the 2000 Act. This code of practice is extended to Scotland in relation to authorisations made under Part II of the 2000 Act which apply to Scotland. A separate code of practice applies in relation to authorisations made under RIP(S)A.

Use of material in evidence

1.9 Material obtained from a source may be used as evidence in criminal proceedings. The proper authorisation of a source should ensure the suitability of such evidence under the common law, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998. Furthermore, the product obtained by a source described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996, where those rules apply to the law enforcement body in question. There are also well-established legal procedures that will protect the identity of a source from disclosure in such circumstances.

2 GENERAL RULES ON AUTHORISATIONS

2.1 An authorisation under Part II of the 2000 Act will provide lawful authority for the use of a source. Responsibility for giving the authorisation will depend on which public authority is responsible for the source.

2.2 Part II of the 2000 Act does not impose a requirement on public authorities to seek or obtain an authorisation where, under the 2000 Act, one is available (see section 80 of the 2000 Act). Nevertheless, where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other lawful authority, the consequences of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

2.3 Public authorities are therefore strongly recommended to seek an authorisation where the use or conduct of a source is likely to interfere with a person's Article 8 rights to privacy by obtaining information from or about a person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

Necessity and Proportionality

2.4 Obtaining an authorisation under the 2000 Act will only ensure that the authorised use or conduct of a source is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for the source to be used. The 2000 Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 29(3) of the 2000 Act.

2.5 Then, if the use of the source is necessary, the person granting the authorisation must believe that the use of a source is proportionate to what is sought to be achieved by the conduct and use of that source. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source 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. The use of a source should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

Collateral Intrusion

2.6 Before authorising the use or conduct of a source, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects 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.

2.7 An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the use and conduct of a source.

2.8 Those tasking a source should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and reauthorised or a new authorisation is required.

2.9 Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the source is being used and of similar activities being undertaken by other public authorities which could impact on the deployment of the source. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a source or of information obtained from that source. In this regard, it is recommended that where the authorising officers in the National Criminal Intelligence Service (NCIS), the National Crime Squad (NCS) and HM Customs and Excise (HMCE) consider that conflicts might arise they should consult a senior officer within the police force area in which the source is deployed. Additionally, the authorising officer should make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

2.10 In a very limited range of circumstances an authorisation under Part II may, by virtue of sections 26(7) and 27 of the 2000 Act, render lawful conduct which would otherwise be criminal, if it is incidental to any conduct falling within section 26(8) of the 2000 Act which the source is authorised to undertake. This would depend on the circumstances of each individual case, and consideration should always be given to seeking advice from the legal adviser within the relevant public authority when such activity is contemplated. A source that acts beyond

the limits recognised by the law will be at risk from prosecution. The need to protect the source cannot alter this principle.

Combined authorisations

2.11 A single authorisation may combine two or more different authorisations under Part II of the 2000 Act. For example, a single authorisation may combine authorisations for intrusive surveillance and the conduct of a source. In such cases the provisions applicable to each of the authorisations must be considered separately. Thus, a police superintendent can authorise the conduct of a source but an authorisation for intrusive surveillance by the police needs the separate authority of a chief constable, and in certain cases the approval of a Surveillance Commissioner will also be necessary. Where an authorisation for the use or conduct of a covert human intelligence source is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State. However, this does not preclude public authorities from obtaining separate authorisations.

Directed surveillance against a potential source

2.12 It may be necessary to deploy directed surveillance against a potential source as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them. An authorisation under this code authorising an officer to establish a covert relationship with a potential source could be combined with a directed surveillance authorisation so that both the officer and potential source could be followed. Directed surveillance is defined in section 26(2) of the 2000 Act. See the code of practice on Covert Surveillance.

Central Record of all authorisations

2.13 A centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for a period of at least three years from the ending of the authorisation.

2.14 Proper records must be kept of the authorisation and use of a source. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a source unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the source. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in the records relating to each source.

2.15 In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation.
- the date and time when any instruction was given by the authorising officer to cease using a source.

2.16 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use made of the source.

Retention and destruction of the product

2.17 Where the product obtained from a source could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

2.18 In the cases of the law enforcement agencies (not including the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

2.19 There is nothing in the 2000 Act which prevents material obtained from properly authorised use of a source being used in other investigations. Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of a source. Authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material.

The Intelligence services, MOD and HM Forces

2.20 The heads of these agencies are responsible for ensuring that arrangements exist to ensure that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.

3 SPECIAL RULES ON AUTHORISATIONS

Confidential Information

3.1 The 2000 Act does not provide any special protection for 'confidential information'. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

3.2 In cases where through the use or conduct of a source it is likely that knowledge of confidential information will be acquired, the deployment of the source is subject to a higher level of authorisation. Annex A lists the authorising officer for each public authority permitted to authorise such use or conduct of a source.

Communications Subject to Legal Privilege

3.3 Section 98 of the 1997 Act describes those matters that are subject to legal privilege in England and Wales. In Scotland, the relevant description is contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995. With regard to Northern Ireland, Article 12 of the Police and criminal Evidence (Northern Ireland) Order 1989 should be referred to.

3.4 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

3.5 The 2000 Act does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and any source which acquires such material may engage Article 6 of the ECHR (right to a fair trial) as well as Article 8. Legally privileged information obtained by a source is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, the mere fact that use has been made of a source to obtain such information may lead to any related criminal proceedings being stayed as an abuse of process. Accordingly, action which may lead to such information being obtained is subject to additional safeguards under this code.

3.6 In general, an application for the use or conduct of a source which is likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstance. Full regard should be had to the particular proportionality issues such a use or conduct of a source raises. The application should include, in addition to the reasons why it is considered necessary for the use or conduct of a source to be used, an assessment of how likely it is that information subject to legal privilege will be acquired. The application should clearly state whether the purpose (or one of the purposes) of the use or conduct of the source is to obtain legally privileged information.

3.7 This assessment will be taken into account by the authorising officer in deciding whether the proposed use or conduct of a source is necessary and proportionate for a purpose under section 29 of the 2000 Act. The authorising officer may require regular reporting so as to be able to decide whether the authorisation should

continue. In those cases where legally privileged information has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material should be made available to him if requested.

3.8 A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, any case where a lawyer is the subject of an investigation or operation should be notified to the relevant Commissioner or Inspector during his next inspection and any material which has been retained should be made available to him if requested.

3.9 Where there is any doubt as to the handling and dissemination of information which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged information, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known to any person whose possession of it might prejudice any criminal or civil proceedings related to the information. Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Communications involving Confidential Personal Information and Confidential Journalistic Material

3.10 Similar consideration must also be given to authorisations that involve confidential personal information and confidential journalistic material. In those cases where confidential personal information and confidential journalistic material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

3.11 Spiritual counselling means conversations between an individual and a Minister of Religion acting in his official capacity, where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

3.12 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.

Vulnerable individuals

3.13 A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances. In these cases, the attached table in Annex A lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a source.

Juvenile sources

3.14 Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. **On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.** In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should be granted by those listed in the attached table at Annex A. The duration of such an authorisation is **one month** instead of twelve months.

4 AUTHORISATION PROCEDURES FOR COVERT HUMAN INTELLIGENCE SOURCES

4.1 Under section 26(8) of the 2000 Act a person is a source if:

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);

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

he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
4.2 A source may include those referred to as agents, informants and officers working undercover.
4.3 By virtue of section 26(9)(b) of the 2000 Act 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.

4.4 By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as mentioned in paragraph 4.1(c) above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.
4.5 The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

4.6 The conduct of a source is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

Authorisation procedures

4.7 Under section 29(3) of the 2000 Act an authorisation for the use or conduct of a source may be granted by the authorising officer where he believes that the authorisation is necessary:
in the interests of national security 1,2;
for the purpose of preventing and detecting 3 crime or of preventing disorder;

in the interests of the economic well-being of the UK;

In the interests of public safety;

for the purpose of protecting public health4;

for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
for any other purpose prescribed in an order made by the Secretary of State5.
4.8 The authorising officer must also believe that the authorised use or conduct of a source is proportionate to what is sought to be achieved by that use or conduct.

4.9 The public authorities entitled to authorise the use or conduct of a source are those listed in Schedule 1 to the 2000 Act. Responsibility for authorising the use or conduct of a source rests with the authorising officer and all authorisations require the personal authority of the authorising officer. An authorising officer is the person designated under section 29 of the 2000 Act to grant an authorisation for the use or conduct of a source. The Regulation of Investigatory Powers (Prescriptions of Offices, Ranks and Positions) Order 2003; SI No: 3171 designates the authorising officer for each different public authority and the officers entitled to act only in urgent cases. In certain circumstances the Secretary of State will be the authorising officer (see section 30(2) of the 2000 Act).

4.10 The authorising officer must give authorisations in writing, except that in urgent cases, they may be given orally by the authorising officer or the officer entitled to act in urgent cases. In such cases, a statement that the

authorising officer has expressly authorised the action should be recorded in writing by the applicant as soon as is reasonably practicable.

4.11 A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making.

4.12 Authorising officers should not be responsible for authorising their own activities, e.g. those in which they, themselves, are to act as the source or in tasking the source. However, it is recognised that this is not always possible, especially in the cases of small organisations. Where an authorising officer authorises his own activity the authorisation record (see paragraphs 2.13 - 2.15) should highlight this and the attention of a Commissioner or Inspector should be invited to it during his next inspection.

4.13 The authorising officers within the police, NCIS and NCS may only grant authorisations on application by a member of their own force, Service or Squad. Authorising officers in HMCE may only grant authorisations on application by a customs officer.

Footnote:

1One of the functions of the Security Service is the protection of national security and in particular the protection against threats from terrorism. These functions extend throughout the United Kingdom, save that, in Northern Ireland, where the lead responsibility for investigating the threat from terrorism related to the affairs of Northern Ireland lies with the Police Service of Northern Ireland. An authorising officer in another public authority should not issue an authorisation under Part II of the 2000 Act where the operation or investigation falls within the responsibilities of the Security Service,as set out above, except where it is to be carried out by a Special Branch or where the Security Service has agreed that another public authority can authorise the use or conduct of a source which would normally fall within the responsibilities of the Security Service.

2HM Forces may also undertake operations in connection with a military threat to national security and other operations in connection with national security in support of the Security Service, the Police Service of Northern Ireland or other Civil Powers.

3Detecting crime is defined in section 81(5) of the 2000 Act.

4This could include investigations into infectious diseases, contaminated products or the illicit sale of pharmaceuticals.

5This could only be for a purpose which satisfies the criteria set out in Article 8(2) of the ECHR.

Information to be provided in applications for authorisation

4.14 In application for authorisation for the use or conduct of a source should be in writing and record:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in section 29(3) of the 2000 Act;
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the purpose for which the source will be tasked or deployed (e.g. In relation to an organised serious crime, espionage, a series of racially motivated crimes etc);

- where a specific investigation or operation is involved, nature of that investigation or operation;
- the nature of what the source will be tasked to do;
- the level of authority required (or recommended, where that is different).
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the authorisation; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

4.15 Additionally, in urgent cases, the authorisation should record (as the case may be):

- the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of a written authorisation was given; and/or
- the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

4.16 Where the authorisation is oral, the detail referred to above should be recorded in writing by the applicant as soon as reasonably practicable.

Duration of authorisations

4.17 A written authorisation will, unless renewed, cease to have effect at the end of a period of twelve months beginning with the day on which it took effect.

4.18 Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy-two hours, beginning with the time when the authorisation was granted or renewed.

Reviews

4.19 Regular reviews of authorisations should be undertaken to assess the need for the use of a source to continue. The review should include the use made of the source during the period authorised, the tasks given to the source and the information obtained from the source. The results of a review should be recorded on the authorisation record (see paragraphs 2.13 - 2.15). Particular attention is drawn to the need to review authorisations frequently where the use of a source provides access to confidential information or involves collateral intrusion.

4.20 In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

Renewals

4.21 Before an authorising officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a source as outlined in paragraph 4.19.

4.22 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of **twelve months**. Renewals may also be granted orally in urgent cases and last for a period of **seventy-two hours**.

4.23 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. The renewal should be kept/recorded as part of the authorisation record (see paragraphs 2.13 - 2.15).

4.24 All applications for the renewal of an authorisation should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in paragraph 4.14;
- the reasons why it is necessary to continue to use the source;
- the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation;
- the tasks given to the source during that period and the information obtained from the conduct or use of the source;
- the results of regular reviews of the use of the source;

Cancellations

4.25 The authorising officer who granted or renewed the authorisation must cancel it if he is satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that satisfactory arrangements for the source's case no longer exist. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer (see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794). Where necessary, the safety and welfare of the source should continue to be taken into account after the authorisation has been cancelled.

MANAGEMENT OF SOURCES

Tasking

4.26 Tasking is the assignment given to the source by the persons defined at sections 29(5)(a) and (b) of the 2000 Act, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

4.27 The person referred to in section 29(5)(a) of the 2000 Act will have day to day responsibility for:

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

4.28 The person referred to in section 29(5)(b) of the 2000 Act will be responsible for the general oversight of the use of the source.

4.29 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a trading standards officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the relevant public authority to determine where, and in what circumstances, such activity may require authorisation.

4.30 It is not the intention that authorisations be drawn so narrowly that a separate authorisation is required each time the source is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may need to be sought.

4.31 It is difficult to predict exactly what might occur each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, the occurrence must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient it should either be updated and reauthorised (for minor amendments only) or it should cancelled and a new authorisation should be obtained before any further such action is carried out.

4.32 Similarly where it is intended to task a source in a new way or significantly greater way than previously identified, the persons defined at section 29(5)(a) or (b) of the 2000 Act must refer the proposed tasking to the authorising officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and the details of such referrals must be recorded.

Management responsibility

- **4.33** Public authorities should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 29(5)(a) and (b) of the 2000 Act for each source.
- **4.34** The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.
- In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.

Security and welfare

4.36 Any public authority deploying a source should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising

officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

4.37 The person defined at section 29(5)(a) of the 2000 Act is responsible for bringing to the attention of the person defined at section 29(5)(b) of the 2000 Act any concerns about the personal circumstances of the source, insofar as they might affect:

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

4.38 Where deemed appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

ADDITIONAL RULES

Recording of telephone conversations

4.39 Subject to paragraph 4.40 below, the interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network may be authorised only by the Secretary of State, in accordance with the terms of Part I of the 2000 Act. Nothing in this code should be taken as granting dispensation from the requirements of that Part of the 2000 Act.

4.40 Part I of the 2000 Act provides certain exceptions to the rule that interception of telephone conversations must be warranted under that Part. This includes, where one party to the communication consents to the interception, it may be authorised in accordance with section 48(4) of the 2000 Act provided that there is no interception warrant authorising the interception. In such cases, the interception is treated as directed surveillance (see chapter 4 of the Covert Surveillance code of practice).

Use of covert human intelligence source with technical equipment

- **4.41** A source, whether or not wearing or carrying a surveillance device and invited into residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or vehicle which take place in his presence. This also applies to the recording of telephone conversations other than by interception which takes place in the source's presence. Authorisation for the use or conduct of that source may be obtained in the usual way.
- **4.42** However, if a surveillance device is to be used, other than in the presence of the source, an intrusive surveillance authorisation and if applicable an authorisation for interference with property should be obtained.

5 OVERSIGHT BY COMMISSIONERS

5.1 The 2000 Act requires the Chief Surveillance Commissioner to keep under review (with the assistance of the Surveillance Commissioners and Assistant Surveillance Commissioners) the performance of functions under Part III of the 1997 Act and Part II of the 2000 Act by the police (including the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police and the Ministry of Defence Police and the British Transport Police), NCIS, NCS, HMCE and of the 2000 Act the other public authorities listed in Schedule 1 and in Northern Ireland officials of the Ministry of Defence and HM Forces

5.2 The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within Part II of the 2000 Act by the Security Service, Secret Intelligence Service (SIS), the Governments Communication Headquarters (GCHQ) and the Ministry of Defence and HM Forces (excluding the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police, and in Northern Ireland officials of the Ministry of Defence HM Forces).

5.3 This code does not cover the exercise of any of the Commissioners' functions. It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

5.4 References in this code to the performance of review functions by the Chief Surveillance Commissioner and other Commissioners apply also to Inspectors and other members of staff to whom such functions have been delegated.

6 COMPLAINTS

6.1 The 2000 Act establishes an independent Tribunal. This Tribunal will be made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.

6.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ
020 7273 4514

Covert Human Intelligence Sources Code of Practice

http://www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codeofpractice/humanintell/index.html

APPENDIX 5 – Home office Draft Code of Practice for the Acquisition and Disclosure of communications Data

Accessing Communications Data Draft Code Of Practice

DRAFT CODE OF PRACTICE – acquisition and disclosure of communications data

Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000

This is a draft code published under section 71(3)(a) of the Regulation of Investigatory Powers Act 2000 and laid before both Houses of Parliament.

Covering Letter

CONTENTS

Footnotes appear at the end of the chapter.

Introduction

1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ("the Act"). It provides guidance on the procedures that must be followed before access to communications data can take place under those provisions.
1.2 The code should be readily available to any members of a public authority who are involved in operations to access communications data.
1.3 The Act provides that the code is admissible in evidence in criminal and civil proceedings. If any provision of the code appears relevant to a question before any court or tribunal hearing any such proceedings, or to the Tribunal established under the Act, or to one of the Commissioners responsible for overseeing the powers conferred by the Act, it must be taken into account.
1.4 This code applies to relevant public authorities as described in Chapter II of Part I of the Act (see para 3.1 below).

1.5 This code **does not** cover conduct consisting in the interception of communications (contents of a communication).
1.6 This code extends to England, Wales, Scotland and Northern Ireland.

General

2.1 The code covers any conduct in relation to a postal service or telecommunication system for obtaining communications data 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, contents of e-mails or interactions with websites. In this code "data", in relation to a postal item, means anything written on the outside of the item.
2.2 A person who engages in such conduct must be properly authorised and must act in accordance with that authority.
2.3 A test of ***necessity*** (see paras 4.1-4.3 below) must be met before any communications data is obtained. The assessment of necessity is one made by a designated person. (This is a person designated for the purposes of Chapter II of Part I of the Act (see para 3.2 below). A designated person has a number of obligations within the provisions of the Act which must be met before communications data is obtained. These are also laid out in this code). A designated person must not only consider it necessary to obtain the communications data but must also consider the conduct involved in obtaining the communications data to be ***proportionate*** (see para 4.4 below) to what it is sought to achieve.

Designated persons within relevant public authorities permitted to access communications data under the Act

3.1 Designated persons within the following "*relevant public authorities*"[1] are permitted under the Act to grant authorisations or serve notices[2], the two routes by which the Act allows communications data to be accessed (see further para 5.1 below):

- a police force (as defined in section 81(1) of the Act);
- the National Criminal Intelligence Service;
- the National Crime Squad;
- HM Customs and Excise;
- the Inland Revenue;
- the Security Service;
- the Secret Intelligence Service;
- the Government Communications Headquarters.

3.2 The appropriate level of official i.e. a designated person within each public authority for granting authorisations or giving notices will be as follows:

- to obtain any communications data defined by section 21(4) of the Act a minimum of Superintendent or equivalent;
- to obtain communications data defined by section 21(4)(c) only of the Act (such as account and subscriber information), a minimum of Inspector or equivalent.)

[1] The Act permits the Secretary of State to add further public authorities to this list by means of an Order subject to the affirmative resolution procedure in Parliament.
[2] The Secretary of State may by Order place restrictions on:

- the authorisations or notices that may be granted or given by designated persons; and
- the circumstances in which, or purposes for which, authorisations or notices may be granted or given.

Relevant public authorities authorised to access communications data from the list in Chapter II of Part I of the Act may be removed, if deemed appropriate, by Order of the Secretary of State.

Purposes for which communications data may be sought

4.1 Under section 22(2) of the Act, communications data may be sought if a designated person believes it is necessary for one or more of the following purposes[3]:

- in the interests of national security;
- for the purpose of preventing or detecting crime or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom (see para 4.2 below);
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

4.2 In exercising his power to grant an authorisation or give a notice in the interests of the economic well-being of the United Kingdom (as provided for by section 22(2)(c)) of the Act, a designated person will consider whether

the economic well-being of the United Kingdom which it is in the interests of is, on the facts of each case, related to State security. The term "State security", which is used in Directive 97/66/EC (concerning the processing of personal data and the protection of privacy in the telecommunications sector), should be interpreted in the same way as the term "national security" which is used elsewhere in the Act and this code. A designated person will not grant an authorisation or give a notice on section 22(2)(c) grounds if this link is not established. Any application for an authorisation or a notice on section 22(2)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of the United Kingdom which it is in the interests of is related to State security on the facts of the case.

4.3 For an action to be necessary in a democratic society the access to communications data must pursue a legitimate aim as listed in para 4.1; fulfil a pressing social need and be proportionate to that aim.

4.4 Under section 22(5) of the Act, a designated person must also consider the conduct involved in obtaining the communications data to be proportionate. Proportionality is a crucial concept. In both the Act and this code reference is made to the conduct being proportionate. This means that even if a particular case which interferes with a Convention right[4] is aimed at pursuing a legitimate aim (as listed in para 4.1 above) this will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any interference with a Convention right should be carefully designed to meet the objective in question and must not be arbitrary or unfair. Even taking all these considerations into account, in a particular case an interference may still not be justified because the impact on the individual or group is too severe.

[3] The Act permits the Secretary of State to add further purposes to this list by means of an Order subject to the affirmative resolution procedure in Parliament.

[4] European Convention on Human Rights (ECHR).

Authorisations and notices

5.1 The Act provides two different ways of authorising access to communications data; through an authorisation under section 22(3) and by a notice under section 22(4). An authorisation would allow the relevant public authority to collect or retrieve the data itself. 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 public authority which served the notice. A designated person decides whether or not an authorisation should be granted or a notice given.

5.2 In order to illustrate, a section 22(3) authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data[5];
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of communications data.

5.3 *Applications for communications data may only be made by persons in the same public authority as a designated person.*

(a) Single points of contact within relevant public authorities

5.4 Notices and where appropriate authorisations for communications data should be channelled through single points of contact within each public authority (unless the exemption in paras 5.13-5.14 applies). This will provide for an efficient regime, since the single points of contact will deal with the postal or telecommunications operator on a regular basis. It will also help the public authority to regulate itself. This will assist in reducing the burden on the postal or telecommunications operator by such requests. Single points of contact will be able to advise a designated person on whether an authorisation or a notice is appropriate.

5.5 Single points 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;
- provide safeguards for authentication;
- assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

(b) Applications to obtain communications data under the Act

5.6 The application form is subject to inspection by the Commissioner and both applicant and designated person may be required to justify their decisions. Applications to obtain communications data under the Act should be made on a standard form (paper or electronic) which must be retained by the public authority (see section 7 of this code) and which should contain the following minimum information:

- the name (or designation) of the officer requesting the communications data;
- 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 (there will also be a

need to identify whether it is communications data under section 21(4)(a), (b) or (c) of the Act);
- the reason why obtaining the requested data is considered to be necessary for one or more of the purposes in paragraph 4.1 above (the relevant purpose also needs to be identified);
- an explanation of why obtaining the data constitutes conduct proportionate to what it seeks to achieve;
    - where appropriate, a consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion is justified; and
- 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 to be included.

5.7 The 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 authorisation or notice.

(c) Considerations for designated person

5.8 A designated person must take account of the following points, so that he is in a position to justify decisions made:

- whether the case justifies the accessing of communications data for one or more of the purposes listed in paragraph 4.1 above, and why obtaining the data is *necessary* for that purpose;
- whether obtaining access to the data by the conduct authorised by the authorisation, or required of the postal or telecommunications operator in the case of a notice, is proportionate to what is sought to be achieved. (A designated person needs to have in mind the conduct which he is authorising or requiring in each case. In making a judgement as to proportionality, a designated person needs to have in mind whether he is granting an authorisation or issuing a notice, and also what the scope of the conduct is. For example, where the conduct covers the provision of ongoing communications data);
    - where appropriate, where accessing the communications data is likely to result in collateral intrusion, whether the circumstances of the case still justify that access; and
- whether any urgent timescale is justified.

(d) Content of an authorisation

5.9 An authorisation itself can only authorise conduct to which Chapter II of Part I of the Act applies. A designated person will make a decision whether to grant an authorisation based upon the application which is made. The application form and the authorisation itself is not served upon the holder of communications data. The authorisation should be in a standard format (written or electronic) which must be retained by the public authority (see section 7 of this code) and must contain the following information:

- a description of the conduct to which Chapter II of Part I of the Act applies that is authorised;
- a description of the required communications data;
- for which of the purposes in paragraph 4.1 above the data is required; and
- the name (or designation) and office, rank or position of the designated person.

5.10 The authorisation should also contain:

- a unique reference number.

(e) Content of a notice

5.11 A designated person will make a decision whether to issue a notice based upon the application which is made. The application form is not served upon the holder of communications data. The notice that they receive contains only enough information to allow them to fulfil their duties under the Act. The notice served upon the holder of the communications data should be in a standard format (written or electronic) which must be retained by the public authority (see section 7 of this code) and must contain the following information:

- a description of the required communications data;
- for which of the purposes in paragraph 4.1 above the data is required;
- the name (or designation) and office, rank or position of the designated person; and
- the manner in which the data should be disclosed.

5.12 The notice should also contain:

- a unique reference number;
- where appropriate, an indication of any urgency;
- a statement stating that data is sought under the provisions of Chapter II of Part I of the Act. i.e. an explanation that compliance with this notice is a legal requirement; and
- contact details so that the veracity of the notice may be checked.

[A specimen copy of a notice can be found at annex A to this code].

(f) Oral authority (urgent cases)

5.13 An application for communications data may only be made and approved orally, on an urgent basis, where it is necessary to obtain communications data for the purpose set out in section 22(2)(g) of the Act[6]:

> "for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health".

5.14 The fact of an oral application and approval must be recorded by the applicant and designated person at the time or as soon as possible. In this case, an authorisation under section 22(3) of the Act must be completed (in a written or electronic format) very shortly thereafter. In the case of a notice under section 22(4) of the Act, a

designated person may make an oral request to a postal or telecommunications operator to disclose communications data which must be followed by a (written or electronic) notice to the postal or telecommunications operator very shortly thereafter. A section 22(4) notice may be issued directly to the postal or telecommunications operator, therefore relaxing the need to do so via a single point of contact.

(g) Disclosure of data

5.15 Notices under section 22(4) of the Act will only require the disclosure of data to:

- the person giving the notice i.e. the designated person; or
- to another specified person who must be from the same relevant public authority. In practice, this is likely to be the single points of contact.

[5] Where possible, this assessment will be based upon information provided by the relevant postal or telecommunications operator.

[6] To give effect to Article 2 (right to life) of the European Convention on Human Rights (ECHR).

Validity of authorisations and notices

(a) Duration

6.1 Authorisations and notices will only be valid for one month. This period will begin when the authorisation is granted or the notice given. A designated person should specify a shorter period if that is satisfied by the request, since this may go to the proportionality requirements. For 'future' communications data disclosure may only be required of data obtained by the postal or telecommunications operator **within** this period i.e. up to one month. For 'historical' communications data disclosure may only be required of data in the possession of the postal or telecommunications operator. A postal or telecommunications operator should comply with a section 22(4) notice as soon as is reasonably practicable. Furthermore, they will not be required to supply data unless it is reasonably practicable to do so.

(b) Renewal

6.2 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.

6.3 A renewed authorisation or notice takes effect at the point at which the authorisation or notice it is renewing expires.

(c) Cancellation

6.4 A designated person shall cancel a notice given under section 22(4) of the Act 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 falls on the designated person who issued it.

6.5 The appropriate level of official within each public authority who may cancel a notice in the event of the designated person no longer being able to perform this duty is to be prescribed by Regulations made under section 23(9) of the Act.

6.6 As a matter of good practice, authorisations should also be cancelled in accordance with the procedure above.

6.7 In the case of a section 22(4) notice, the relevant postal or telecommunications operator will be informed of the cancellation.

Retention of records by public authorities

7.1 Applications, authorisations and notices for communications data must be retained by the relevant public authority until it has been audited by the Commissioner. The public authority should also keep a record of the dates on which the authorisation or notice is started and cancelled.

(a) Errors

7.2 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 is practical.

7.3 Applications must also be retained to allow for the complaints Tribunal, under Part IV of the Act, to carry out its functions.

7.4 This code does not affect any other statutory obligations placed on public authorities to retain data under any other enactment. (Where applicable, in England and Wales, the relevant tests given in the Criminal Procedures and Investigations Act 1996[7], namely whether any material gathered might undermine the case for the prosecution against the accused, or might assist the defence, should be applied).

(b) Data protection safeguards

7.5 Communications data, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the Data Protection Act 1998[8] and its data protection principles should be adhered to.

[7] Further guidance is available in the CPIA code of practice.

[8] Further guidance is available from http://www.homeoffice.gov.uk/foi/datprot.html

Oversight

8.1 The Act provides for an Interception of Communications Commissioner whose remit is to provide independent oversight of the use of the powers contained within Part I.

8.2 This code does not cover the exercise of the Commissioner's functions. However, it will be the duty of any person who uses the powers conferred by Chapter II of Part I to comply with any request made by the Commissioner to provide any information he requires for the purposes of enabling him to discharge his functions.

Complaints

9.1 The Act establishes an independent Tribunal, which is made up of senior members of the legal profession or judiciary and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction.
9.2 This code does not cover the exercise of the Tribunal's functions. However, details of the relevant complaints procedure should be readily available, for reference purposes, at public offices of those public authorities permitted to access communications data under the provisions of Chapter II of Part I of the Act. Where this is not possible, copies should be made available by post or e-mail.

Annex A to draft code of practice

Unique reference number: [*to be completed by the public authority*]
[*an indication of any urgency*]

NOTICE UNDER SECTION 22(4) OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000 REQUIRING COMMUNICATIONS DATA TO BE OBTAINED AND DISCLOSED

To: [NAME OF POSTAL OR TELECOMMUNICATIONS OPERATOR and address].
In accordance with section 22(4) of the Regulation of Investigatory Powers Act 2000, I hereby require you -
*(a) if not already in possession of the data to which this notice relates, to obtain it; and {*for use in those cases where you are actually asking for data to be captured for the duration of the notice - this should be omitted where you are only requiring the disclosure of historical data*}.
(b) to disclose all communications data to which this notice relates, whether in your possession or subsequently obtained by you.

Description of communications data to which this notice relates:

[*enter details of the communications data required {distinguish here between data (a) to be obtained if not already in the possession of the operator (omitting if not relevant) and (b) to be disclosed - each should be described separately*}].
*(a) [*communications data to be obtained*];
(b) [*communications data to be disclosed*].
This notice is valid from [*start date – issue date of this notice*] to [*end date*]. – This must be no more than one month from the date of this notice, or earlier if cancelled under section 23(8)). This notice may be renewed at any time before the end of the period of one month starting with [*issue date*] by the giving of a further notice.
I believe that it is necessary for this communications data to be obtained:
[***List the purpose(s) that the communications data is required for (from Section 22(2)) - follow the statutory language exactly)***].
In reaching this conclusion I have satisfied myself that obtaining this data by the conduct required by this notice is proportionate to what is sought to be achieved by so obtaining the data.
You are required to produce the said communications data to [*specify the person (a name or designation must be specified), office, rank or position to whom the data is to be disclosed*] of [*public authority*] for him to take away as specified below:
[***Specify the manner in which the data is to be disclosed***].
Date .....…….....
Designated Person (a minimum of Superintendent or equivalent. For communications data falling under section 21(4)(c) of the Act, a minimum of Inspector or equivalent): [***Enter office, rank or position***] ……...….
This notice may be verified by contacting the following:
[*enter contact details i.e. of the Single Point of Contact*]
*Omit as appropriate

APPENDIX 6 - CCTV policy in relation to RIPA

Appendix H Regulation of Investigatory Powers Act

Guiding Principles

Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act 2000 came into force on 2nd October last. It relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:-

*Subject to subsection (6), surveillance is directed for the purposes of this Part 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 specifically identified for the purposes of the investigation or operation); and

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

CCTV being used intrusively will be authorised other than by this section of the RIP Act. Appropriate guidelines already exist for intrusive surveillance.

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases, this will fall into sub section **c** above, i.e. it will be an immediate response to events or circumstances. In this case, it would not require authorisation unless it were to continue for some time. The code says some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authority will almost certainly be required.

Slow time requests are authorised by a Superintendent or above.

If an authority is required immediately, an Inspector may do so. The forms in both cases must indicate the reason and should fall within one of the following categories:-

An authorisation is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) in the interests of the economic well-being of the United Kingdom;

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or

(g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then in writing by way of the forms. Any authority given should be recorded appropriately for later reference.

This should include the name of the officer authorising.

Examples:

Insp. Authorisation

An example of a request requiring Inspector authorisation might be where a car is found in a car park late at night and known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Where crime squad officers wish to have a shop premises monitored from the outside, which is suspected of dealing in stolen goods over a period of days.

No Authorisation

Where officers come across a local drug dealer sitting in the town centre/street and wish to have the cameras monitor them, so as not to divulge the observation taking place.

APPENDIX 7 - S.I. 2010/123

This Order has been made in substitution of S.I. 2009/3404 and is being issued free of charge to all known recipients of that instrument.

S T A T U T O R Y I N S T R U M E N T S

2010 No. 123

INVESTIGATORY POWERS

The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010

Made - - - -	*22nd January 2010*
Laid before Parliament	*26th January 2010*
Coming into force - -	*18th February 2010*

The Secretary of State, in exercise of the powers conferred by sections 29(2)(c) and (7)(b) and 43(8) of the Regulation of Investigatory Powers Act 2000(**a**), makes the following Order:

PART 1

GENERAL

Citation and commencement

1. This Order may be cited as the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 and shall come into force on 18th February 2010.

Interpretation

2.—(1) In this Order—

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

"matters subject to legal privilege" means (subject to paragraph (2)) matters to which section 98(2), (3) or (4) of the Police Act 1997(**b**) applies;

"private information" has the meaning given in section 26(10) of the 2000 Act; and

"source" means covert human intelligence source.

(2) For the purposes of this Order—

(a) communications and items are not matters subject to legal privilege when they are in the possession of a person who is not entitled to possession of them, and

(b) communications and items held, or oral communications made, with the intention of furthering a criminal purpose are not matters subject to legal privilege.

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

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

PART 2
CONDUCT TO WHICH THIS ORDER APPLIES

Matters subject to legal privilege

3.—(1) This Order applies where any conduct that is, or is to be, authorised in an authorisation under section 29 of the 2000 Act consists in any activities involving conduct of a source, or the use of a source, to—

(a) obtain matters subject to legal privilege,

(b) provide access to any matters subject to legal privilege to another person, or

(c) disclose matters subject to legal privilege.

(2) Subject to paragraph (3), an authorisation for conduct to which this Order applies shall not be granted or renewed unless it satisfies the requirements imposed by Part 3.

(3) Where a single authorisation under section 29 of the 2000 Act authorises conduct to which this Order applies and other conduct falling within Part II of that Act, the requirements imposed by Part 3 of this Order shall only apply in relation to those parts of the combined authorisation which authorise conduct falling within paragraph (1).

PART 3
APPROVAL BY ORDINARY SURVEILLANCE COMMISSIONER OR SECRETARY OF STATE

Approving officer

4.—(1) Where the person designated for the purposes of section 29 of the 2000 Act is—

(a) a member of any of the intelligence services,

(b) an official of the Ministry of Defence,

(c) an individual holding an office, rank or position in Her Majesty's Prison Service or the Northern Ireland Prison Service, or

(d) a member of Her Majesty's forces, the approving officer for the purposes of this Part shall be the Secretary of State.

(2) In any other case, the approving officer shall be an ordinary Surveillance Commissioner.

Notification

5.—(1) Before a person grants or renews an authorisation for conduct to which this Order applies, that person shall, in accordance with arrangements made by the relevant approving officer, give notice to the approving officer.

(2) A notice under this article—

(a) shall be given in writing to the relevant approving officer,

(b) shall state that the approval of an approving officer is required by article 6 before the authorisation is granted or renewed, and

(c) shall include the matters specified in paragraph (3) or, as the case may be, paragraph (4).

(3) Where a person gives notice under paragraph (1) seeking approval to grant an authorisation, the notice to the approving officer shall, in addition to the statement required by article 5(2)(b), specify—

(a) the grounds on which the person giving the notice believes the matters specified in article 6(4) and section 29(2)(b) and (c) of the 2000 Act;

(b) the conduct falling within article 3(1) that is, or is to be, authorised by the authorisation;

(c) the identity, where known, of—

(i) the professional legal adviser and his client or any person representing his client, or

(ii) the professional legal adviser or his client or any such representative and any other person, to whom the activities of the source relate;

(d) the matters subject to legal privilege (to the extent known) to which the conduct that is to be authorised by the authorisation relate; and

(e) whether the conduct to be authorised by the authorisation is likely to result in the obtaining of private information about any person who is not specifically identified in the notice for the purposes of the investigation or operation.

(4) Where a person gives notice under paragraph (1) seeking approval to renew an authorisation, the notice to the approving officer shall, in addition to the statement required by article 5(2)(b), specify—

(a) whether the authorisation is being renewed for the first time, or, where it has been previously renewed, each occasion on which it has been renewed;

(b) the matters required by paragraph (3), as they apply at the time of the notice seeking approval to renew;

(c) every respect (if any) in which the information contained in the previous notice under this article has changed;

(d) the reason why it is considered necessary to renew the authorisation;

(e) the content and value to the investigation or operation of the matters subject to legal privilege obtained from the conduct or the use of the source in the period since the grant of the authorisation;

(f) the results of any reviews of the matters mentioned in section 43(7) of the 2000 Act; and

(g) the period for which the authorisation is considered likely to continue to be necessary.

(5) Any notice that is required by this article to be given in writing may be given, instead, by being transmitted by electronic means.

Approval required for grant or renewal of authorisations

6.—(1) An authorisation for conduct to which this Order applies shall not be granted or renewed until—

(a) it has been approved in accordance with this article by the relevant approving officer, and

(b) written notice of the approving officer's decision to approve the grant or renewal of the authorisation has been given, in accordance with paragraph (3)(b), to the person who gave notice under article 5.

(2) Where an approving officer receives a notice under article 5, the approving officer shall as soon as is reasonably practicable—

(a) scrutinise the authorisation, and

(b) decide whether or not to approve the grant or renewal of the authorisation.

(3) The approving officer shall—

(a) give his approval to the grant or renewal of the authorisation if, and only if, the approving officer is satisfied that there are reasonable grounds for believing that—

(i) the authorisation is necessary on grounds falling within paragraph (4), and

(ii) the requirements of section 29(2)(b) and (c) of the 2000 Act are satisfied in the case of the authorisation; and

(b) give written notice of his decision to the person who gave notice under article 5 as soon as reasonably practicable after making that decision.

(4) An authorisation is necessary on grounds falling within this paragraph if it is necessary—

(a) in the interests of national security;
(b) for the purpose of preventing or detecting serious crime; or
(c) in the interests of the economic well-being of the United Kingdom;

(5) Any notice that is required by this article to be given in writing may be given, instead, by being transmitted by electronic means.

Notices given by the Secretary of State

7.—(1) Subject to paragraph (2), a notice of the Secretary of State's decision to approve the grant or renewal of an authorisation under article 6(3)(b) shall not be given except under the hand of the Secretary of State.

(2) In an urgent case in which—

(a) approval has been sought for the grant or renewal of an authorisation for conduct to which this Order applies by a member of any of the intelligence services, and
(b) the Secretary of State has expressly authorised the giving of the notice in that case, the notice may be given under the hand of a senior official.

PART 4
DURATION OF AUTHORISATIONS

Duration

8.—(1) Subject to paragraph (2), where an authorisation authorises conduct to which this Order applies, section 43(3) of the 2000 Act shall have effect as if the period specified in paragraph (b) of that subsection was—

(a) six months in the case of an authorisation which was granted or renewed by a member of any of the intelligence services; and
(b) three months in any other case.

(2) Where an authorisation—

(a) was granted by a member of any of the intelligence services pursuant to a notice given in accordance with articles 6(3)(b) and 7(2) under the hand of a senior official, and
(b) has not been renewed pursuant to a notice given in accordance with articles 6(3)(b) and 7(1) under the hand of the Secretary of State, section 43(3) of the 2000 Act shall have effect as if the period specified in paragraph (b) of that subsection was the end of the second working day following the day of the grant or, as the case may be, renewal of the authorisation.

PART 5
REVOCATION

Revocation

9. The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2009(**a**) is revoked.

Home Office
22nd January 2010

David Hanson
Minister of State

EXPLANATORY NOTE

(This note is not part of the Order)

Section 29 of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act") makes provision for the granting of authorisations for the conduct or the use of a covert human intelligence source. This Order exercises the power conferred on the Secretary of State by section 29(2)(c) and (7)(b) to impose additional requirements that must be satisfied before an authorisation is granted (or renewed) under that section.

Part 2 of the Order describes the conduct or uses of covert human intelligence sources to which the additional requirements apply. Article 3(1) provides that the Order applies where the conduct that is, or is to be, authorised in an authorisation under section 29 of the 2000 Act consists in any activities involving conduct of a source, or the use of a source, to obtain, provide access to or disclose matters subject to legal privilege. Article 3(2) prohibits the granting or renewal of authorisations for conduct of this description unless the requirements imposed by Part 3 are satisfied. Where an authorisation authorises conduct to which the Order applies and other conduct falling within Part II of the 2000 Act, article 3(3) confirms that the requirements imposed by Part 3 only apply in relation to those parts of the combined authorisation which authorise conduct falling within article 3(1).

Part 3 of the Order creates an enhanced regime of prior approval for conduct to which the Order applies. Article 6 provides that such an authorisation cannot be granted or renewed until it has been approved either (as specified in article 4) by the Secretary of State or by an ordinary Surveillance Commissioner ("the approving officer"). The approving officer may only give his approval if satisfied that there are reasonable grounds for believing that the authorisation is necessary in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom, and the requirements of section 29(2)(b) and (c) of the 2000 Act are satisfied. Article 7 makes provision for the giving of notices by the Secretary of State under article 6.

Part 4 of the Order exercises the power conferred on the Secretary of State by section 43(8) of the 2000 Act to shorten the period at the end of which an authorisation of a specified description is to cease to have effect. Article 8 exercises this power with regard to section 43(3)(b) of the 2000 Act so that, subject to paragraph (2), an authorisation that authorises conduct to which the Order applies ceases to have effect after six months rather than twelve in the case of an intelligence service authorisation, and three months instead of twelve months in any other case. Paragraph (2) limits the duration of urgent intelligence services authorisations which have not been renewed pursuant to a notice given under the hand of the Secretary of State to the end of the second working day following the day of the grant or renewal of the authorisation.

(**a**) S.I. 2009/3404.

This Order has been made in substitution of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2009 (S.I. 2009/3404)

Part 5 of this Order revokes the earlier instrument.

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Carol Tullo, Controller of Her Majesty's Stationery Office and Queen's Printer of Acts of Parliament.

This Order has been made in substitution of S.I. 2009/3404 and is being issued free of charge to all known recipients of that instrument.

S T A T U T O R Y I N S T R U M E N T S

2010 No. 123

INVESTIGATORY POWERS

The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010

£5.50

E5833 1/2010 105833T 19585