APPENDIX 1

HILLINGDON
LONDON

REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY

TABLE OF CONTENTS

To be inserted when policy approved by Cabinet

PART A: INTRODUCTION

A1. Introduction

The Regulation of Investigatory Powers Act 2000 (RIPA) is wide ranging in its application and impacts on all officers with an enforcement or investigatory capacity, including internal investigations.

The London Borough of Hillingdon is committed to implementing RIPA in a manner that is consistent with the spirit and letter of RIPA and the HRA. The London Borough of Hillingdon is committed to conducting all relevant actions in a manner which strikes a balance between the rights of the individual and the legitimate interests of the public.

This policy aims to provide a framework to control and supervise covert activities such as directed surveillance and the use of CHIS in criminal investigations. It aims to balance the need to protect the privacy of individuals against the enforcement functions exercised by the London Borough of Hillingdon. This policy will be reviewed on an annual basis by Cabinet.

The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this Document should contact, at the earliest opportunity, the London Borough of Hillingdon's Senior Responsible Officer for advice and assistance. Where necessary, appropriate training and development will be facilitated by the Senior Responsible Officer.

A copy of this Document and related Forms has been placed on the Council's Intranet. This will be regularly updated.

A2. The Scope of this Policy

Any employee / contractor / agent of the London Borough of Hillingdon must apply for authorisation to conduct covert surveillance. The surveillance is to be necessary and proportionate for the purposes of the prevention and

detection of crime or the prevention of disorder and if it is likely that private information about a person will be obtained.

When carrying out covert surveillance on members of the public as part of its enforcement responsibilities, the London Borough of Hillingdon is acting as a public authority. This means that RIPA and this policy apply to the covert surveillance being undertaken.

The London Borough of Hillingdon may carry out two types of covert surveillance:

1. Directed Surveillance
2. Use of a Covert Human Intelligence Source (CHIS)

In cases where an employee of the London Borough of Hillingdon is under internal investigation, the Council's role is that of an employer and not a public authority. RIPA does not apply in these cases unless the employee is under investigation for a criminal offence. In such a scenario, the Council must comply with RIPA if the surveillance evidence is to be admissible in criminal proceedings.

A3. Effective Date

This policy will come into effect on 06 April 2010. After this date, only the procedures contained in this document will be permissible.

It will be the responsibility of Directors to ensure their relevant members of staff are also suitably trained as "Applicants'.

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

A4. Legal Framework

The Human Rights Act 1998 brought into law many of the provisions of the 1950 European Convention on Human Rights and Fundamental Freedoms (ECHR). Article 8 requires the Council to have respect for people's private and family lives, their homes, and their correspondence. These rights can be referred to as "Article 8 rights".

The Human Rights Act 1998 makes it unlawful for any local authority to act in a way which is incompatible with the ECHR. However these are not absolute rights and are qualified by the ability of the Council to interfere with a person's Article 8 rights if:-

Such interference is in accordance with the law
Is necessary
And is proportionate

Any covert surveillance activity carried out by a local authority must meet the above 3 requirements in order to ensure that surveillance does not breach Article 8 rights.

When we talk of interference being "in accordance with the law", this means that any such interference is undertaken in accordance with national legislation. Within England, Wales and Northern Ireland, **the legislation governing covert surveillance is Regulation of Investigatory Powers Act 2000(RIPA) and its associated Codes of Practice.**

Necessity - covert surveillance shall only be undertaken where it is designed to prevent or detect crime and/or the Prevention of disorder. The only reason for which directed surveillance may be necessary to the Council is for the purpose of preventing or detecting crime and/or the prevention of disorder.

Proportionality - the use and extent of covert surveillance must be in proportion to the significance of the matter being investigated.

The concepts of necessity and proportionality are discussed in detail further in the document in relation to applications for directed surveillance and CHIS.

Statutory Codes of Practice supplement RIPA. These deal respectively with covert surveillance and property interference, Directed Surveillance and CHIS, interception of communications, communications data and electronic information.

The Council's policy recognises the important role these Codes of Practice play in the practical implementation of RIPA. The Council will conduct all of its activities relating to RIPA in accordance with the Codes of Practice. It is essential, therefore, that all relevant officers involved in RIPA are familiar with these Codes of Practice.

The Codes of Practice deal with the use of Covert Surveillance and the use of persons such as informants and Undercover Officers (CHIS) who gather information in a covert capacity. There are separate codes of practice covering Covert Surveillance and property surveillance CHIS and Directed Surveillance. Copies of the relevant codes are on Horizon.

RIPA also applies to the Accessing of Communications Data. The Council has produced separate guidance dealing with the accessing of communications data under the SPOC (Single Point of Contact) provisions.

The Council has numerous statutory duties and powers to investigate the activities of private individuals and organisations within its jurisdiction for the benefit and protection of the greater public. Some of these investigations may require surveillance or the use of directed surveillance or a Covert Human Information Source (CHIS). Officers seeking to use powers under RIPA will clarify whether they are undertaking directed surveillance or making use of a Covert Human Information Source (CHIS).

Surveillance investigations may include benefit fraud; environmental health; housing; planning and criminal investigations.

However a considerable amount of observations are carried out in an overt capacity by Council employees carrying out their normal functions such as parking enforcement, general patrolling etc. Where surveillance activities are general and routine and do not involve the systematic and planned surveillance of an individual, a RIPA authorisation will not be necessary. RIPA is not designed to prevent these routine activities.

A5. Consequences of Non-Compliance

The use of covert surveillance will most likely result in officers obtaining private information about individuals, or groups of individuals. Private information is defined in section 26(10) of RIPA 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. The Codes of Practice have now extended the definition of private information to encompass aspects of family and professional or business relationships.

Where Investigators obtain private information without first obtaining the relevant RIPA authorisation (where it is a requirement that such authorisation be obtained), the information obtained may be regarded as a breach of Article 8 rights and therefore excluded under Section 78 of the Police and Criminal Evidence Act 1984. Should the evidence be disallowed by a court, the prosecution case may be lost with a financial cost to the Council.

The person who was the subject of the surveillance may in turn complain to the Investigatory Powers Tribunal - who may order the London Borough of Hillingdon to pay compensation. The activity may also be challenged through the civil courts under the Human Rights Act 2000 for breach of privacy.

PART B: Surveillance

B1. Covert Surveillance

Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

Overt surveillance takes place where the surveillance is not hidden, such as alerting the public to the use of CCTV in a public place. Overt surveillance does not require authorisation.

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

The use of overt CCTV cameras by public authorities does not normally require an authorisation under the 2000 Act. Members of the public will be aware that such systems are in use, and their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008, issued by the Information Commissioner's Office. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under the 2000 Act.

However, where overt CCTV or ANPR cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the

definition of directed surveillance. The use of the CCTV or ANPR system in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

Covert surveillance is where the person or people under observation are not aware that surveillance is taking place. ***Covert surveillance can only be justified where other investigation methods would not obtain the necessary evidence.***

Any officer considering undertaking covert surveillance must maintain a record of any considerations with regard to private information, necessity and proportionality.

Private information is defined in section 26(10) of RIPA 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. The Codes of Practice have now extended the definition of private information to encompass aspects of family and professional or business relationships.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of **private information**. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by the Council of that person's activities for future consideration or analysis.

Where covert surveillance activities are unlikely to result in the obtaining of private information about a person, or where there is a separate legal basis for such activities, neither the 2000 Act nor this code need apply.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of

behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be considered appropriate.

Directed surveillance is covert in nature but is not intrusive. This means that it does not involve entry or surveillance inside a private residence or vehicle.

Surveillance is directed surveillance if the following are all true:

- it is covert, but not intrusive surveillance;
- it is conducted for the purposes of a specific investigation or operation;
- it 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);
- it is conducted 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.

An authorisation for directed or intrusive surveillance is only appropriate for the purposes of a specific investigation or operation, insofar as that investigation or operation relates to the grounds specified at Section 28(3) of the 2000 Act. The Investigatory Powers Tribunal has clarified that Covert surveillance for any other general purposes should be conducted under other legislation, if relevant, and an authorisation under Part II of the 2000 Act should not be sought.

Thus, the planned covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if **such surveillance is likely** to result in the obtaining of private information about that, or any other person.

It is emphasised that **Private information** may include but is not limited to personal data, such as names, telephone numbers and address details. Where private information is acquired by means of covert surveillance of a person having **a reasonable expectation of privacy**, a directed surveillance authorisation is appropriate.

Where overt surveillance equipment is used in a pre-planned manner to support a specific or targeted investigation and private information is likely to be obtained; a Directed Surveillance Authorisation is appropriate. It is clarified that "Hot-Spot" surveillance must be considered subjectively in order to determine whether a directed surveillance authorisation is appropriate.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be considered appropriate.

For the purposes of the 2000 Act, residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. This specifically includes hotel or prison accommodation that is so occupied or used.15 However, common areas (such as hotel dining areas) to which a person has access in connection with their use or occupation of accommodation are specifically excluded.

Examples of residential premises would therefore include:

- *a rented flat currently occupied for residential purposes;*

- *a prison cell (or police cell serving as temporary prison accommodation);*
- *a hotel bedroom suite.*

Examples of premises which would not be regarded as residential premises would include:

- *a communal stairway in a block of flats (unless known to be used as a temporary place of abode, by for example a homeless person);*
- *a prison canteen or police interview room*
- *a hotel reception area or dining room;*
- *the front garden or driveway of premises readily visible to the public;*
- *residential premises occupied by a public authority for non-residential purposes.*

A private vehicle is defined in the 2000 Act as any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This would include, for example, a company car, owned by a leasing company and used for business and pleasure by the employee.

Recording of or listening to telephone conversations or interception of post may be authorised as directed surveillance where one party (either the sender or recipient) to the communication consents to the interception. Such surveillance may be authorised in accordance with Section 48(4) of the RIPA which provides that in such cases, the interception is treated as directed surveillance.

Directed Surveillance undertaken by or on behalf of the London Borough of Hillingdon must be authorised according to the processes laid out in this document.

The Council Officers can use Directed Surveillance IF, AND ONLY IF, RIPA procedures, detailed in this policy document are followed.

Intrusive surveillance is covert surveillance which is carried out with or without a recording device in relation to anything taking place on any residential premises or in a private vehicle and involves the presence of an individual or device.

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.

The London Borough of Hillingdon will not authorise intrusive surveillance.

B2. Covert Human Intelligence Source (CHIS)

A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However, the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as CHIS.

Under section 26(8) of the RIPA a person is CHIS if:

A. He establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (B) or (C);

B. He covertly uses such a relationship to obtain information or to provide access to any information to another person; or

C. He covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

The word "establishes" when applied to a relationship means "set up". It does not require, as "maintains" does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity. Officers engaging in test purchases are required to document whether the test purchase activity gives rise, in their opinon, to a relationship. Where it does give rise to a relationship, a CHIS or Directed Surveillance authorisation may be necessary. Officers are advised that a CHIS authorisation will be required when test purchase activity involves the use of a recording device.

By virtue of section 26(9)(b) of RIPA, 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.**

By virtue of section 26(9) (c) of RIPA, a relationship is used covertly, and information obtained as 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.**

Juvenile CHIS - Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. **Only the Chief Executive and the Borough Solicitor acting jointly are duly authorised by the Council to use Juvenile Sources**, as there are other

onerous requirements for such matters. (Refer to CHIS Code of Practice, paragraph 3.14)

Vulnerable Individuals - 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 herself, or unable to protect himself or herself against significant harm or exploitation.

A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. **Only the Chief Executive and the Borough Solicitor acting jointly are duly authorised by the Council to use Vulnerable Individuals**, as there are other onerous requirements for such matters.

B2.1 Conduct and Use of a CHIS

The use of a CHIS 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.

Conduct of a CHIS includes establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.

Use of a CHIS details the actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

The use of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.5 In general, therefore, an authorisation for use of a CHIS will be necessary to authorise steps taken by a public authority in relation to a CHIS.

Care should be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant applications, reviews, renewals and cancellations are correctly performed. A CHIS may in certain circumstances be the subject of different use or conduct authorisations obtained by one or more public authorities. Such authorisations should not conflict with each other.

Tasking a person to obtain information covertly may result in authorisation under Part II of the 2000 Act being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

This will be likely to be the case where a member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance may need to be considered where there is an interference with the Art 8 rights of an individual

When completing applications for the use of a CHIS you are stating who the CHIS is, what they can do and for which purpose.

The Council can use a CHIS IF, AND ONLY IF, RIPA procedures, detailed in this policy document are followed.

B2.2 Management of CHIS

Any surveillance operation involving a CHIS must include:

A. a person who has the day to day responsibility for dealing with the CHIS and for the CHIS' security and welfare (**Handler**)
B. at all times there will be another person who will have general oversight of the use made of the CHIS (**Controller**)
C. at all times there will be a person who will have responsibility for maintaining a record of the use made of the CHIS

The Handler will have day to day responsibility for:

A. dealing with the CHIS on behalf of the authority concerned;
B. directing the day to day activities of the CHIS;
C. recording the information supplied by the CHIS; and Monitoring the CHIS' security and welfare;

The Controller will be responsible for the general oversight of the use of the CHIS. The Controller will usually be one management tier above the Handler in order to ensure that strategic control of the operation is retained.

B2.3 Tasking

Tasking is the assignment given to the CHIS by the Handler or Controller by, 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 CHIS 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.

A CHIS may wear or carry a surveillance device for the purpose of recording information. The CHIS may not leave devices on the premises after they have departed, as this would constitute intrusive surveillance.
In some instances, the tasking given to a person will not require the CHIS to establish a personal or other relationship for a covert purpose. For example a CHIS may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council 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 Council to determine where, and in what circumstances, such activity may require authorisation.

Should a CHIS authority be required all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice

Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises should constitute directed surveillance (see paragraph 12 below), unless it is done overtly. For example, it will only be possible to record without authorisation if the noisemaker is warned in advance.

However, it should be noted that the London Borough of Hillingdon considers that recording sound with a DAT recorder on private premises would

constitute **intrusive surveillance** if the DAT recorder could pick up conversations from the target premises of the same quality as if it had been placed inside the target premises.

Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will require prior directed surveillance authorisation.

B2.4 Management Responsibility

All Officers of the London Borough of Hillingdon involved in a CHIS operation must ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be necessary the CHIS Codes of Practice should be consulted to ensure that the Council can meet its management responsibilities.

B2.5 Security and Welfare

The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the CHIS. 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 CHIS of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset.

B3. Compulsory Considerations for Directed Surveillance and CHIS

B3.1 Necessity and Proportionality

Obtaining an RIPA 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. It must be necessary for the **prevention and**

detection of crime or of preventing disorder. It must also be shown the reasons why the requested activity is necessary in the circumstances of that particular case. The key question to be asked is: Is there any alternative to surveillance which will satisfy the objective? If the response is a positive one, then the use of RIPA cannot be justified unless pressing circumstances exist which prevent the use of the alternative option.

Then, if the activities are **necessary**, the person granting the authorisation must believe that the activities are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the subject and others who might be affected by it against the need for the activity in operational terms.

An authorisation will not be proportionate if the surveillance is considered excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be addressed in any application for covert surveillance:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- evidencing what other methods had been considered and why they were not implemented.

B3.2 Collateral Intrusion

Collateral Intrusion is intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation as neighbours or other members of the subject's family. Efforts to reduce the collateral intrusion should be undertaken.

Prior to and during any authorised RIPA activity, a risk assessment should take place to identify any collateral intrusion and take continuing precautions to minimise the intrusion where possible. The collateral intrusion, the reason why it is unavoidable and precautions to minimise it will have to be detailed on any relevant application forms.

Before authorising surveillance the Authorising Officer should take into account the risk of collateral intrusion detailed on the relevant application forms.

The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but officers should weigh up the importance of the activity to be carried out in operational terms on the one hand and the risk of collateral intrusion on the other hand.

B3.3 Unexpected Interference with Third Parties

When officers are carrying out covert directed surveillance or using a CHIS, officers should inform the Authorising Officer if the 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.

B3.4 Confidential Information

Confidential information consists of matters subject to Legal Privilege, confidential personal information or confidential journalistic material and applications where there is a likelihood of acquiring such information **can only be authorised by the Borough Solicitor or the Legal Services Office Managing Partner.**

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. Journalistic material is also mentioned in the codes however it is highly unlikely that this will be obtained. The definition should it be required can be obtained from the Codes of Practice at section 3.10.

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

Those handling material from such operations should be alert to anything which may fall within the definition of confidential material. Confidential material should not be retained or copied unless it is necessary for a specified purpose;

Confidential material should be disseminated only where an appropriate officer (having sought advice from the Borough Solicitor) 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;

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

B3.5 Working With/Through Other Agencies

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

When some other agency (e.g. Metropolitan Police Services):

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

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

In terms of option (a) above, if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

If in doubt, please contact the Senior Responsible Officer at the earliest opportunity.

Part C: Obtaining RIPA Authorisations

C1. Authorisation Procedures

Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 1** provides a flow chart of process from application consideration to recording of information. Note that the procedure detailed applies to Directed Surveillance and CHIS operations.

C2. Senior Responsible Officer

The Senior Responsible Officer will act as a central co-ordinator for the Council's RIPA activities.

The Senior Responsible Officer will:

a. Primarily ensure that the Council's surveillance activities conform to RIPA legislation including any urgent remedial action that must be taken to ensure compliance with the Codes;

b. Ensure that the Council's policy conforms to RIPA and remains fit for purpose;

c. Provide advice and guidance to officers with regard to RIPA related queries;

d. Review authorisations granted in order to ensure compliance with the legislation and policy. Where relevant, the SRO may as a result of the review, suggest to the relevant Member(s) further action /improvements or changes that need to be made;

e. Direct any remedial action that needs to be taken urgently by a Directorate / officer/ team in order to ensure compliance;

f. Ensure that the training needs of officers are met and where necessary, set out a regular programme of training.

C3. Authorised Officers

Forms can only be signed by Authorised Officers who have been confirmed by the Borough Solicitor or his representative. Authorised posts are listed in **Appendix 2**. This Appendix will be kept up to date by the Senior Responsible Officer.

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire.

No covert surveillance using RIPA should be undertaken at any time unless it has been **authorised in writing on the appropriate form by a designated Authorised Officer.**

Only the Borough Solicitor or Legal Services Office Managing Partner may authorise covert surveillance involving a Juvenile CHIS and/or Vulnerable Individuals.

The authorisations do not lapse with time. An application to cancel the authorisation must be submitted by the Applicant Officer. Applicant officers must ensure that reviews, cancellations or renewals of authorisations must be submitted to the Authorising Officer on or before the date specified by the Authorising Officer.

The Authorising Officer may unilaterally cancel a covert surveillance authorisation in the event that an application for review, cancellation or renewal is not submitted to the Authorising Officer on or before a specified date.

In such circumstances, the Applicant officer will be instructed to **cease all surveillance immediately**. Failure to comply with this instruction may lead to action against the Applicant Officer. Nothing in the preceding paragraph shall prevent an Applicant Officer from re-applying for authorisation for covert surveillance where an authorisation was unilaterally cancelled by the Authorising Officer. In such a situation, the procedure outlined in Appendix 1 must be adhered to.

C4. Grounds for Authorisation

Directed Surveillance or the Conduct and Use of the CHIS can only be authorised by the authorising officers for preventing or detecting crime or the prevention of disorder.

The onus is on the Authorising Officer to ensure that the surveillance meets the tests of **necessity and proportionality**.

C5. ASSESSING THE APPLICATION

An Authorising Officer should consider all information provided on the Application form and if necessary ask for further information from the Investigating Officer. When completing the form, the Authorising Officer should write down exactly what they are authorising. All authorities must be signed, showing the date and time the authority was granted.

Before an Authorising Officer signs a Form, **s/he must**:-

(a) Be mindful of this Corporate Policy & Procedures Document, the training provided by the Borough Solicitor and any other guidance issued, from time to time, by the Borough Solicitor on such matters;

(b) Satisfy him/herself that the RIPA authorisation is:-

(i) **In accordance with the law**;

(ii) **Necessary** in the circumstances of the particular case on one of the grounds mentioned in paragraph 9 above; **and**

(iii) **Proportionate** to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information. **Officers must be aware that the least intrusive method will be considered proportionate by the courts**.

(d) Take into account the risk of intrusion into the privacy of persons other then the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

(e) set a date for review of the authorisation at least once every calendar month (or at shorter intervals, depending on the circumstances of the particular case).

(f) Ensure that any RIPA Departmental Register and the Central Register are duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Borough Solicitor's

Central Register, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.**

When authorising the conduct or use of a CHIS, the Authorising Officer **must also:-**

(a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

(b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

(e) ensure records contain particulars and are not available except on a need to know basis

C6. Urgent Authorisations

Urgent authorisations should not normally be necessary, but a verbal authorisation can be given if the time which would elapse before written authorisation can be granted would be likely to endanger life or jeopardise the investigation.

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.

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. It will not be a case of urgency where the officer has simply forgotten about the requirement for authorisation.

An urgent oral authorisation may be granted by Authorising Officers detailed in **APPENDIX 2.**

Urgent authorisations must be followed by a formal written application form at the earliest possible opportunity and the relevant section completed by the Authorising Officer justifying the oral authorisation. **This completed form must be submitted to the Authorising Officer.**

C7. Duration of Applications

Directed Surveillance	3 Months
Urgent Oral Authority	72 Hours
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Juvenile Sources	1 Month
Urgent Oral Authority	72 Hours
Renewal	12 months

All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire.

Part D: APPLICATION FORMS

The Borough Solicitor and/or the Senior Responsible Officer shall regularly advise officers of the forms to be completed. These forms will also be placed on the Council Intranet for officers to complete.

D1. Applying for Authorisation

All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments for

CHIS operations should take place prior to the completion of the application form and **must** be attached to the completed form.

An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference (see collateral intrusion on page 19). The Authorising Officer will take this into account, particularly when considering the proportionality of the directed surveillance or the use of a CHIS.

All applications will be submitted to the Authorising Officer.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, it must be noted that the application for the use of a CHIS can include instructions for directed surveillance. In such a situation, it will be necessary to complete a CHIS form only. Officers must ensure that the request for Directed Surveillance required is included in the CHIS Application Form.

Applications will be issued with a unique reference number by the Senior Responsible Officer, taken from the next available number in the Central Record of Authorisations.

D2. Reviews

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. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

In each case the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each

application. However reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably a new application form may be more appropriate. You do not have to wait until the review date if it is being submitted for a change in circumstances.

Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time. **Failure to submit a review form punctually may result in the unilateral cancellation of the authorisation by the Authorising Officer.**

D3. Renewal

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. Renewals may also be granted orally in urgent cases and last for a period of seventy-two hours.

An application for renewal should not be made until shortly before the authorisation period is drawing to an end. A renewal takes effect on the day on which the authorisation would have ceased.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed

unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

D4. Cancellation

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.

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision on the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraphs 2.14 - 2.15 in the Codes of Practice).

PART E: Documentation and Central Record

E1. Central Record

Authorising Officers or Managers of relevant enforcement departments must keep appropriate records to administer and manage the RIPA application process. The Originals of any application form will be held by the Senior Responsible Officer as part of a centrally retrievable record.

A centrally retrievable record of all authorisations will be held by the Senior Responsible Officer and regularly updated whenever an authorisation is granted, reviewed, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for at least

six years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater. Key information from this record shall be captured on a spreadsheet containing the following information:

A. The type of authorisation;
B. The date the authorisation was given;
C. Name and rank/grade of the authorising officer;
D. The unique reference number (URN) of the investigation or operation;
E. The title of the investigation or operation, including a brief description and names of subjects, if known;
F. Whether the urgency provisions were used, and if so why.
G. Record of the result of each review of the authorisation;
H. If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
I. Whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
J. The date the authorisation was cancelled.
K. Authorisations by an Authorising Officer in urgent cases where they are directly involved in the investigation or operation (see Authorising Officer Responsibility page 17.) If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

As part of the Central Record the Senior Responsible Officer will also retain:

A. The original of each application, review, renewal and cancellation together with any supplementary documentation of the approval given by the Authorising Officer
B. A record of the period over which the surveillance has taken place;
C. The frequency of reviews prescribed by the Authorising Officer;

D. A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
E. The date and time when any instruction was given by the Authorising Officer.

For CHIS applications the Codes state;

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

A. The original authorisation form together with any supplementary documentation and notification of the approval given by the Authorising Officer;
B. The original renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
C. The reason why the person renewing an authorisation considered it necessary to do so;
D. Any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
E. Any risk assessment made in relation to the source;
F. The circumstances in which tasks were given to the source;
G. The value of the source to the investigating authority;
H. A record of the results of any reviews of the authorisation;
I. The reasons, if any, for not renewing an authorisation;
J. The reasons for cancelling an authorisation.
K. The date and time when any instruction was given by the Authorising Officer to cease using a source.

E2. Storage and Retention of Surveillance Material

All material obtained and associated with an application will be subject of the provisions of the Criminal Procedures Investigations Act 1996 (CPIA) Codes of Practice which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances.

It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of the Data Protection Act. All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

If legal proceedings have been instituted, material must remain in secure storage for six (6) years after the accused is acquitted or convicted. Where a decision is taken not to institute prosecution action, material must be destroyed 6 months after such a decision is taken.

Each relevant service within the Council may have its own provisions under their Data Retention Policy which will also need to be consulted to ensure that the data is stored in a secure manner until such time as it is destroyed.

E3. Training

There will be an ongoing training programme for Council Officers who will need to be aware of the impact and operating procedures with regards to RIPA. The Senior Responsible Officer will be required to retain a list of all those officers who have received training and when the training was delivered.

It will be the responsibility of Directors and Deputy Directors to ensure their relevant members of staff are also suitably trained as "Applicants' so as to avoid common mistakes appearing on Forms for RIPA authorisations.

Authorising Officers must have received formal RIPA training before being allowed to consider applications for surveillance and CHIS.

E4. Surveillance Equipment – Control/Inventory

It is the responsibility of the Service Head to ensure the issue and use of any equipment held by the service for the purpose of conducting covert directed surveillance (e.g. radios, cameras, etc) is correctly recorded and usage is

subject to audit. The Senior Responsible Officer shall compile a central inventory of all equipment held or arrangements made by the London Borough of Hillingdon with third parties for the purpose of conducting covert surveillance.

E5. Complaints Procedures

The Council's Complaints Procedure may be used for any complaint, regarding breach of this Policy and Guidance.

E6. Further Information

This Policy, relevant forms and London Borough of Hillingdon guidance notes for completion for applications, renewals, cancellations and reviews of Directed Surveillance and use of Covert Human Intelligence Sources shall be placed on the London Borough of Hillingdon intranet for reference purposes. In addition, the RIPA Officer may be contacted when and as necessary.

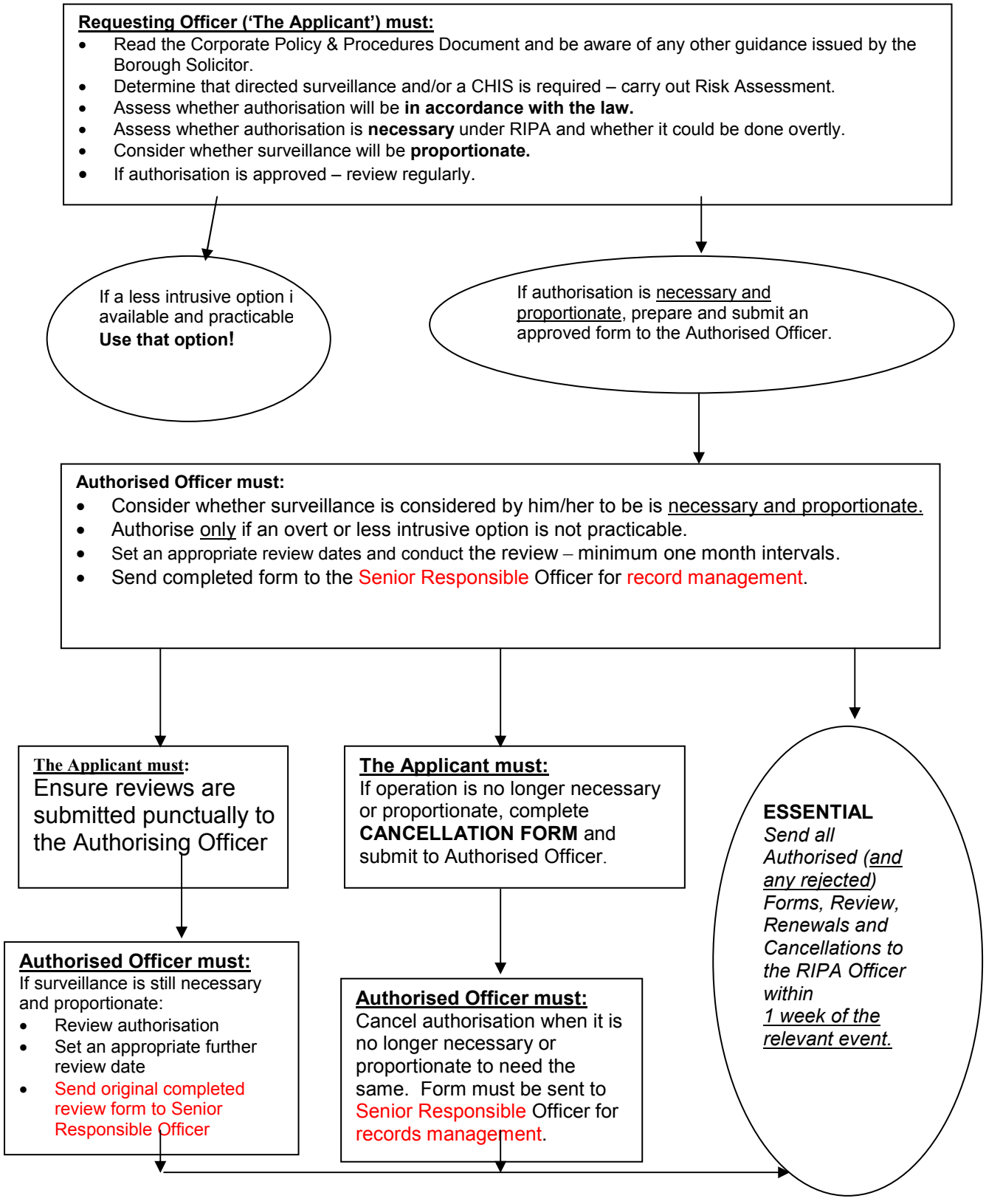
The Statutory Codes of Practice that supplement RIPA are available on the following web link:

http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/

Although the Codes of Practice do not have the same force as RIPA, they augment and expand on its implementation. Officers must always ensure that enforcement activities comply with the Codes of Practice.

APPENDIX 1

RIPA FLOW CHART



NB: If in doubt, ask the Senior Responsible Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

Appendix 2

List of Authorising Officers and authorising levels

Name	Area	Contact Number	Level of Surveillance Authority			
			Juvenile or Vulnerable CHIS and/or Confidential Material from CHIS or Directed Surveillance	CHIS	Directed Surveillance	Oral
Kathryn Sparks	Environment and Consumer Protection	Ext 7501	No	Yes	Yes	Yes
Rajesh Alagh	Borough Solicitor	Ext 0617	Yes	Yes	Yes	Yes
Glen Egan	Legal Services Office Managing Partner	Ext 7602	Yes	Yes	Yes	Yes
Senior Responsible Officer						
Glen Egan	Legal Services Office Managing Partner	Ext 7602	Yes	Yes	Yes	Yes