REGULATION OF INVESTIGATORY POWERS POLICY UPDATE

Cabinet Member	Councillor Scott Seaman-Digby
Cabinet Portfolio	Cabinet Member for Co-ordination and Central Services
Officer Contact	Beejal Soni, Deputy Chief Executive's Office
Papers with report	Appendix 1 – Regulation of Investigatory Powers Act Policy and Procedure Appendix 2 – Acquisition of Communication Data Policy

HEADLINE INFORMATION

Purpose of report	This report provides Members with and update to the Council's procedures with regard to the Regulation of Investigatory Powers Act 2000 (RIPA). This report also seeks approval for a revised policy and procedures on the exercise of the Council's powers under RIPA. This report further seeks approval for a policy with regard to the Acquisition Communications Data under RIPA.
Contribution to our plans and strategies	Does this report contribute to delivering any plan or strategy of the council, if so state which here.
Financial Cost	The revised policies set out in this report do not have any financial implications for the Council.
Relevant Policy Overview Committee	Corporate Services and Partnerships
Ward(s) affected	All

RECOMMENDATIONS

That Cabinet:

1. **Approve the revised Regulation of Investigatory Powers Act 2000(RIPA) Policy and Procedures;**
2. **Approve the new Acquisition of Communication Data Policy;**
3. **Request that the Leader of the Council be notified within 24 hours of any application for surveillance being granted;**
4. **Agree that relevant details (excluding any sensitive information) of all surveillance applications approved annually under The Regulation of Investigatory Powers Act 2000 be published on the Council Website from May 2010 and;**
5. **Agree that the Council's RIPA policy be reviewed on or before December 2010.**

INFORMATION

Reasons for recommendation

In June 2008, the London Borough of Hillingdon was inspected by the Office of Surveillance Commissioner (OSC) to review the Council's management of covert activities. This coincided with significant public debate in the last year on the way local authorities have applied RIPA. The inspection resulted in numerous recommendations to improve the Council's use and procedures with regard to RIPA. The inspection also coincided with increased public concern about the use, by Local Authorities, of RIPA. Consequently, it was decided to review and amend the existing RIPA Corporate Policy and Procedure in order to consolidate the OSC recommendations and address public concerns about local authority use of RIPA. The result is a revised RIPA policy founded on accountability and regular evaluation of surveillance powers. Cabinet is therefore requested to consider and approve the amended policy attached at Appendix A.

Part 1 Chapter II of the Regulation of Investigatory Powers Act 2000 governs what and how external communications data can be used by local councils in the course of investigation work. As part of the review and amendment of the existing Corporate Policy and Procedure with regard to RIPA, it was agreed to provide a framework for officers seeking to make use of the powers with regard to external communications. Cabinet is requested to consider and approve the Acquisition of Communication Data Policy attached at Appendix B.

Alternative options considered / risk management

Not to adopt the recommended policies - Failure to approve the revised Regulation of Investigatory Powers Act 2000 Policy and Procedure may lead to the Council not fully complying with the legislation and accompanying Codes of Practice. This in turn may render evidence obtained inadmissible in court. Failure to take action on the Office of Surveillance Commissioner's recommendations may lead to public criticism of the London Borough of Hillingdon.

A failure to adopt a Policy to acquire communications data in accordance with the Regulation of Investigatory Powers Act 2000 may expose the Council to legal challenge under the Human Rights Act, when seeking to use evidence obtained using these powers. The Council can also be fined by the Interception of Communication Commissioner for failing to comply with the Home Office Code of Practice on the Acquisition of Communications Data.

Comments of Policy Overview Committee(s)

None

Supporting Information

1. RIPA is divided into 5 parts:

    a. Part I - Interception of communications / Accessing Communications Data;
    b. Part II- Intrusive and Directed Surveillance / Conduct of a Human Information Source (CHIS)
    c. Part iii - Investigation of electronic data protected by encryption
    d. Part iv - Oversight mechanism / complaints procedure and Codes of Practice
    e. Part v - Miscellaneous

2. The RIPA Codes of Practice clarify and introduce regulations to update the use of covert surveillance and the interception of communications law enforcement agencies. It aimed to ensure that these investigation powers were used in accordance with the Human Rights Act and take into account technological advances.

3. In the main, local authority powers are exercised under Part 1 (which came into effect on 5 January 2004) and Part II (which came into effect on 25 September 2000).

4. The Council's current RIPA Policy and Procedure was adopted by Cabinet, on 4 September 2003. In April 2006, the Council was inspected by the Office of Surveillance Commissioners and changes to the existing policy were recommended.

5. On 23rd June 2008, the Council was once again inspected by the Office of Surveillance Commissioners. Having noted the progress made with regard to amending the existing policy and procedures; the following recommendations were made:

   a. The existing RIPA Policy and Procedures document be reviewed as previously recommended;
   b. That a single electronic central record be created and maintained to monitor RIPA Applications and their progress;
   c. That guidance and policy relating to proportionality and collateral intrusion be specifically addressed;
   d. That the process of reviewing and cancelling RIPA applications be reconsidered in order to ensure that Authorising Officers retained control of the process;
   e. That arrangements be documented for dealing with the product of covert surveillance;
   f. That the latest Home Office forms be adopted by the London Borough of Hillingdon.

6. In December 2008, the Office of Surveillance Commissioners released a document detailing recommendations for policy and procedures for any public authority seeking to utilise RIPA powers.

7. The recent Home Office consultation on RIPA Codes of Practice also provided a further indication of likely changes to the existing Codes of Practice.

8. In response to this consultation, a decision was taken to designate the Chief Executive Officer and Deputy Chief Executive Officer as Counter-signing officers on all RIPA surveillance applications in order to ensure that the Council used its RIPA powers in proportionate manner.

9. The revised policy brings into effect the recommendations made by the Office of Surveillance Commissioners in 2006 and 2008 and clarifies the application process.

10. The revised policy details the following changes:

    a. A central record comprising an electronic and paper record has been set up and will be maintained by Legal Services;
    b. The policy provides better guidance on key concepts such as "necessity", "proportionality", "collateral intrusion" and the distinction between public and private places.

c. Explains the legal framework relating to the operation of RIPA including the consequences of not acting in accordance with the Policy;
d. Discusses in detail the RIPA process including review processes to regularly assess surveillance;
e. Discusses the retention, storage and destruction of surveillance material;
f. Creates a central log of all surveillance equipment held by Council
g. Ensures accountability by ensuring that the Chief Executive or Deputy Chief Executive approve ALL RIPA applications in advance of the surveillance taking place. The Chief Executive or Deputy Chief Executive will also countersign reviews / renewals / cancellations of RIPA authorisations.

Acquisition of Communications Data

11. The provisions of Part I, Chapter II of the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Communications Data) Order 2003 (SI2003/3172) came into force on 5 January 2004.

12. Communications data encompasses communications using the postal service, fixed line phones, mobile phones, internet and emails. The Act entitles Local authorities to request certain data from communication providers as part of an investigation which purpose is for the "prevention and detection of crime or prevention of disorder".

13. The nature of the data that can be obtained by a Local Authority is restricted and notably does not include the content of a communication. However the Local Authority may request information such as details of the registered owner of a specific telephone number or a date when billing information and addresses were amended. This data could be useful in certain investigations, such as benefit fraud. For example, establishing the name and address of a subscriber to a mail redirection service will help confirm a change of address or status.

14. As from 1 April 2005, Local Authorities that want to make use of these powers can only do so if they have established one or more officers to act as their Single Point of Contact (SPoC). The role of the SPoC is "to enable and maintain effective co-operation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data".

15. The SPoCs are also expected to promote good practice and provide informed advice to both the Applicant and the Authorising Officer to ensure only practical and lawful data requests are made.

16. The SPoC has to be registered with the Home Office and attend and pass an accredited SPoC course. A list of SPOCs within the London Borough of Hillingdon is attached as part of the policy document.

17. In order to ensure that the use of these powers comply with the recommended Home Office Code of Practice and is not subject to legal challenge, a policy and procedure must apply to the use of these powers.

18. The attached Communications policy and procedures has been developed for this purpose, and is subject to the Cabinet's approval. The policy explains:

a. What types of surveillance come within the ambit of the Communications Data Policy;
b. When it will be appropriate for the Council to make use of such powers;
c. The role of the named officers acting as a SPOC during the process;
d. The procedure to be followed to apply for, renew or cancel requests for Communications Data;
e. The records which should be kept relating to Communications Data applications.

19. The policy is based on the provisions of RIPA, the relevant Home Office Code of Practice and guidance provided by the Information Commissioner. It will provide greater clarity to officers whilst ensuring the Council has in place a proper control mechanism for the use of these powers.

Financial Implications

17. The attached policies do not have any financial implications for the Council.

EFFECT ON RESIDENTS, SERVICE USERS & COMMUNITIES

What will be the effect of the recommendation?

The policies will contribute to creating a safer Borough by ensuring that officers can successfully undertake enforcement action. The Policies will also reassure residents of the Residents of the London Borough of Hillingdon that the Council takes very seriously the implications of making use of powers under RIPA and will only make use of such powers where no alternative option is available.

Consultation Carried Out or Required

None

CORPORATE IMPLICATIONS

Corporate Finance

A Corporate Finance officer has reviewed the report and is satisfied that the policies do not have any financial implications for the Authority.

Legal

The purpose of the Regulation of Investigatory Powers Act, 2000 ("RIPA") is to consolidate the law on the use of investigatory powers, to monitor investigative procedures more effectively and to ensure that these powers are used in accordance with human rights.

Human Rights legislation requires the Council to respect the private and family life of citizens, their home and their correspondence. However, this is a qualified right and interference is permissible if it is:

- in accordance with the law
- necessary, and
- proportionate.

The Act provides a statutory framework within which Council staff can, in carrying out their proper duties, interfere with the qualified right to privacy enjoyed by citizens. However, unless correct procedures are followed, evidence may later be disallowed in Court, a complaint could be made to the Ombudsman and the Council might be ordered to pay compensation. In any event, such matters would not promote the Council's reputation and would be likely to attract adverse press and media interest.

The adoption of both policies will ensure compliance with the legislation and Codes of Practice relating to RIPA. It will also provide tangible evidence of the Council's desire to achieve best practice standards by compliance with the recommendations of the statutory oversight bodies.

The Cabinet collectively is responsible for decisions which have a significant impact on two or more wards where the outcome will have a significant impact on the wellbeing of the community or the quality of service provided to a significant number of people living or working in an area.

Corporate Property

Not applicable

Relevant Service Groups

Not applicable

BACKGROUND PAPERS

The Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers (Communications Data) Order 2003 (SI2003/3172)

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 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 therefore be reviewed at regular intervals by the Legal Services section.

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 RIPA officer for advice and assistance. Where necessary, appropriate training and development will be facilitated by the RIPA 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

RIPA would therefore apply to any employee / contractor / agent of the London Borough of Hillingdon seeking to conduct covert surveillance on condition that the surveillance is undertaken only for the purposes of the prevention and detection of crime or the prevention of disorder.

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.

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

The existing Corporate Policy and Procedures for the Regulation of Investigatory Powers Act 2000 came into effect on 31 December 2003.

This policy will replace the existing policy. This policy will come into effect on 21 October 2009. After this date, only the procedures contained in this document will be permissible.

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.

Authorised Officers must also ensure that staff who report to them follow this Corporate Policy & Procedures Document 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.

Necessity - covert surveillance shall only be undertaken where it is designed to achieve a legitimate objective. The only reasons for which directed surveillance may be necessary to be carried out by the Council under this legislation are: -
Preventing or detecting crime
Prevention of disorder

Proportionality - the use and extent of covert surveillance shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated.

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)**

Statutory Codes of Practice supplement RIPA. These deal respectively with covert surveillance, 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 whilst having due regard to and whilst following the recommended practice of the Codes of Practice. It is essential, therefore, that all relevant officers involved in RIPA are familiar with the content of 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 two separate codes of practice, relevant to this policy covering Covert Surveillance and CHIS.

RIPA also applies to the Accessing of Communications Data under Part 1, Chapter 2 of the legislation. 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 by audit such as fraud offences.

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. These activities are general and routine and do not involve the systematic surveillance of an individual. RIPA is not designed to prevent these activities or regulate them.

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.

If Investigators undertake covert activity to which RIPA applies without properly obtained authorisation, 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 Ombudsman 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 can involve monitoring, observing or listening to people. This includes their movements, conversations, activities or other communications or recording anything with a surveillance device.

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.

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***

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. Directed Surveillance 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 (**not a business) – whether or not they are the target of the investigation/operation, and

C. is not carried out in immediate response to events or circumstances, which make prior authorisation not reasonably practical.

Recording of or listening to telephone conversations or interception of post may be authorized 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 authorized according to the processes laid out in this document.

The Council 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 authorize 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.

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.

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 recording sound (with a DAT recorder) on private premises would constitute intrusive surveillance if the DAT recorder could pick up sound from the target premises of the same quality as if it had been placed in the target premises.

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

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. The interference with the person's right to privacy should be no greater than that which is required to meet the aim and objectives.

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 AND the Countersigning Officer.**

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 <u>on behalf of the Council</u> 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 RIPA 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 RIPA 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. Authorised Officers

Forms can only be signed by Authorised Officers who hold a Certificate from the Borough Solicitor or his representative. Authorised posts are listed in **Appendix 2**. This Appendix will be kept up to date by the Borough Solicitor or Legal Services Office Managing Partner and added to as needs require. The Borough Solicitor has been duly authorised to add, delete or substitute posts listed in Appendix 2.

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 **authorized in writing on the appropriate form by a designated Authorised Officer AND the**

Countersigning Officer. The authorisation of the Countersigning Officer is not required for an urgent oral authorisation.

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

The authorisations do <u>not</u> 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 Countersigning Officer may unilaterally cancel a covert surveillance authorisation in the event that an application for review, cancellation or renewal is not submitted to the Authorizing 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 Countersigning Officer. In such a situation, the procedure outlined in Appendix 1 must be adhered to.

C3. Grounds for Authorisation

Directed Surveillance or the Conduct and Use of the CHIS can only be authorised by the authorizing 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**.

C4. 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. **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

C5. 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. **The express authorisation of the Counter-Signing Authorising Officer will not be required for urgent oral authorisations.**

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 and Counter-Signing Authorising Officer for authorisation.**

C6. 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. (see cancellations page 12)

Part D: APPLICATION FORMS

The Borough Solicitor and/or the RIPA 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. Following completion of the application, the Authorising Officer shall submit the form to the Counter-Signing Authorising Officer to perform a quality check of the application.

The application will only be regarded as authorised when it is signed by BOTH the Authorising Officer and Counter-Signing 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 RIPA 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 Countersigning 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 may keep whatever records they see fit to administer and manage the RIPA application process. The Originals of any application form will be held by the RIPA Officer as part of a centrally retrievable record.

A centrally retrievable record of all authorisations will be held by the RIPA 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. A 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 RIPA 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 RIPA 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 RIPA Officer shall retain 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.

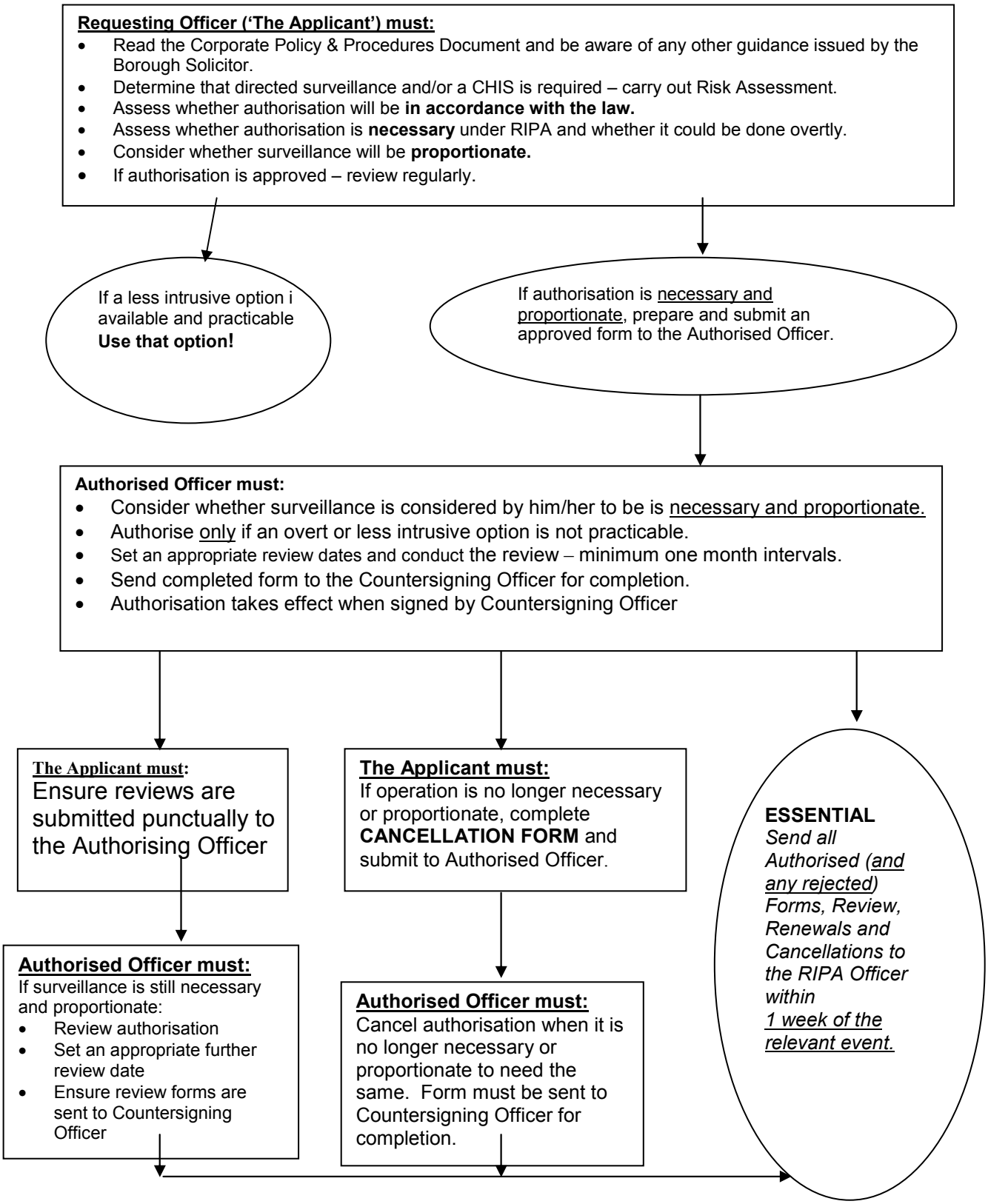
E6. Further Information

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. Annex 5 provides a summary of the key areas of which officers should be aware

APPENDIX 1
RIPA FLOW CHART



NB: If in doubt, ask the RIPA 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
Christopher Norris	Adult Social Care Health and Housing	Ext 0889	No	Yes	Yes	Yes
Rajesh Alagh	Borough Solicitor	Ext 0617	Yes	Yes	Yes	Yes
Glen Egan	Legal Services Practice Manager	Ext 7602	Yes	Yes	Yes	Yes
Countersigning Officers						
Hugh Dunnachie	Chief Executive	Ext 0569	Yes	Yes	Yes	No
Fran Beasley	Deputy Chief Executive	Ext 8344	Yes	Yes	Yes	No
RIPA Officer						
Beejal Soni	Licensing Lawyer	Ext 6425	No	No	No	No

APPENDIX 2

HILLINGDON
LONDON

ACQUISITION OF COMMUNICATIONS DATA POLICY

CONTENTS PAGE

To be completed when content is approved by Cabinet

A. INTRODUCTION AND KEY MESSAGES

1. This Corporate Policy and Procedures document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 ("RIPA") and the Home Office Guidance on the Acquisition and Disclosure of Communications Data Code of Practice October 2007. The Council takes responsibility for ensuring the Procedures are continuously improved.

2. The authoritative position on communications data 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 Council's Borough Solicitor for advice and assistance.

3. Appropriate training and development will be organised by the Legal Services Department for relevant authorised officers and other Senior Managers.

B. COUNCIL POLICY STATEMENT

1. The Council takes seriously its statutory responsibilities and will, at all times, act in accordance with the law and take necessary and proportionate action in these types of matters. In that regard, the Borough Solicitor is duly authorised by the Council to keep this document up to date and to amend, delete, add or substitute relevant provisions as necessary. For administration and operational effectiveness, the Borough Solicitor is also authorised to add or substitute all officers authorised for the purpose of this policy.

2. It is essential that all activities of this nature, whether they will lead to prosecution or not, are carried out in accordance with this Code of Practice and Policy. Investigations which are not authorised could leave the Council open to legal challenge by individuals who consider that there has been an intrusion of their privacy.

3. The purpose of this document is to reinforce the requirements of the Act and the Code of Practice, to ensure compliance with the Act, to protect the rights of individuals and to minimise the risk of legal challenge as a result of officer actions.

C. EFFECTIVE DATE OF OPERATION

1. This Policy is operational forthwith, replacing any previous policy and procedures with regard to the acquisition of communications data. It will apply to all Council staff and Contractors employed by the Council. All relevant Council Contracts will include a term that this Policy and the Council's associated procedures are to be observed by any contractor operating on behalf of the Council.

2. A copy of this policy document together with the Home Office Codes of Practice and the Investigatory Powers Tribunal leaflets will be made available for public inspection at the Council offices (Legal Services Section) as well as on the Council's internet site.

D. GENERAL INFORMATION ON COMMUNICATIONS DATA

1. Communications Data transactions involve:

    - the postal service
    - e-mails (incoming and outgoing)
    - internet (browsing or site hosting)
    - fixed line telephone calls

- mobile telephone calls

2. The legislation empowers public bodies to require Communication Service Providers (CSPs) like British Telecom, to provide the public body with communication data if the appropriate process is followed.

3. The CSP can levy a charge for the costs they incur in providing the information in accordance with the published scale of charges. The cost of acquiring the data should therefore be weighed against the benefit it will provide.

4. Local Councils are classified as Part 3 Public Authorities which means that there are limits on what data we are permitted to acquire as summarised in the table below.

	RIPA TERM	MEANING	EXAMPLE
Allowed	Subscriber Data [Section 21(4)(c)]	Information about the person who subscribes to/uses the communication service	Name and address of the user of a phone number
Allowed	Service use Data [Section 21(4)(b)]	Information about the use made of the communication service	Telephone numbers called and duration of calls
Not allowed	Traffic Data [Section 21(4)(a)]	Information about how the communication was transmitted	Location of a mobile phone when communication was sent
Not allowed	Interception Data [RIPA Part 1 – Chapter 1]	The content of the communication	The content of the phone conversation

5. The policy provides a more detailed breakdown of the process of acquiring various types of communication data from a communication service provider.

6. This policy does not apply to internal communication systems that have no connection with the external sites (For example, internal e-mails and telephone calls).

E. WHAT THIS POLICY DOES AND DOES NOT DO

- Local Authorities are allowed to access service data and subscriber data but only for the prevention or detection of crime or the prevention of disorder.

- Local Authorities do require prior authorisation for obtaining communications data.
- Local Authorities do require safeguards for the conduct and use of the acquisition of communications data.

F. CATEGORIES OF COMMUNICATIONS DATA

There are three broad areas of communications data, only two of which can be accessed by this Council. Further, the powers awarded to local authorities do not permit access to the contents of the communication itself.

They are as follows:

1. `Section 21(4)(b) Service Use Data

– this is information held by a telecom or postal service provider about the use made of a service by a person under investigation such as:

- Outgoing calls on a landline telephone or contract or pre-pay mobile telephone
- Timing and duration of service usage
- Itemised connection records
- Internet log-on history
- E-mails (sent)
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring
- Information about the provision and use of forwarding/redirection services (postal and telecom)
- Information about selection of preferential numbers or discount calls
- Records of postal items, for example records of registered/recorded/special delivery postal item, record of parcel consignment/delivery/connection

2. Section 21(4) (c) Subscriber Data

- This is information about Communication Service Users such as:

- Name of account holder/subscriber (also known as “reverse lookups”)
- Installation and billing addresses
- Method of payments/billing arrangements
- Collection/delivery arrangements for a PO box (i.e. whether it is collected or delivered – not where it is collected from or whom it is delivered to)
- Information about apparatus used by or made available to the account holder/subscriber including the manufacturer model etc.
- Other customer information example accounts notes, demographic information or sign up data (not passwords or personalised access information)

Local Authorities are not authorised to obtain access to “Traffic Data” i.e. Information that identifies any person, equipment, location to or from which communication is or maybe transmitted.

G. ORGANISATIONS FROM WHICH LOCAL AUTHORITIES MAY ACCESS COMMUNICATIONS DATA

All communications data is accessed from Communication Service Providers (CSP's).

These may include (but are not limited to):

- **Telecom providers:** Mobile telephone service providers, landline telephone service providers or international simple voice resellers
- **Internet providers** : ISP's, virtual ISP's and Portholes
- **Postal providers:** Royal Mail

H. THE PERSONNEL INVOLVED IN THE ACQUISITION OF COMMUNICATIONS DATA

1. **Applicant:**

The applicant is any officer of the Council involved in conducting an investigation and who makes an application to a designated person, in writing or electronically, for authorisation to access communications data.

Officers contemplating seeking authorisation should first discuss the proposed application with their line manager. Various options for obtaining the information required other than by using covert techniques, should be explored. It maybe valuable at this stage to discuss the content, scope and aims of the application with the SPOC before completing and submitting any formal application.

If a decision is made to continue then the applicant must complete the application form setting out, for consideration by the designated person, certain information including:

- the purpose for which the data is required;
- the nature of the enquiry;
- the details of the data required;
- the timescale in which the data is needed.

The applicants must also state in the application why the request for authorisation is necessary and proportionate, and outline any potential collateral intrusion arising from the request and what steps are being taken reasonably to minimise any such intrusion.

The application form must be given a unique identifying number by the RIPA Officer. The form should then be submitted to the SPOC.

2. **The Single Point of Contact (SPOC).**

All SPOC officers will have attended a Home Office approved course and passed an examination at the end of this course. Accredited officers are granted a unique SPOC Personal Identification Number (PIN) for their tenure with the Council as SPOC. Details of accredited SPOCS must be made available to CSPs for authentication purposes. SPOC details shall also be held by central records for reference purposes.

The SPOC will act as a conduit between the applicant, designated person and CSP in any application in order to ensure consistency in dealings with various CSPs.

Authorised SPOCs are referred to in Appendix 1.

The responsibilities and role of the SPOC are as follows:

- To assess whether access to communications data in a particular case is reasonably practical for the CSP;
- To advise Applicants and the Designated Person on the practicalities of accessing different types of communications data some different Communication Service Providers (CSP)
- To advise Applicants and the Designated Person on whether specific communication data falls under Section 21(4)(b) or Section 21(4)(c) of RIPA
- To assess any cost and resource implementations for both the Council and the CSP
- When applications are approved by the Designated Person, the SPOC shall forward the Notice to the CSP, file all original documents, forward original documents to central records for monitoring purposes and forward relevant documents and responses to the Applicant and Designated Person;
- To provide a safeguard for CSP's that authorisations and Notices are authentic
- To keep abreast on any developments relating to accessing communications data;
- To develop policies and strategies to make effective and lawful use of legislation in order to support operations
- To maintain and keep up-to-date a SPOC log sheet for applications

The SPOC will, in essence, assess the application and in particular whether the request has been made properly and whether the required communications data can reasonably be obtained together with any adverse cost or resource implications. To this end, the SPOC is required to document and maintain full records of any comments / discussions / queries related to each application.

3. The Designated Person (DP)

A Designated Person must hold the rank or grade of an Assistant Chief Officer, an Assistant Head of Service, a Service Manager or equivalent and must have current working knowledge of Human Rights principles. A DP has been so designated for the purposes of acquiring communications data by the order. A list of designated persons is referred to in Appendix 1.

The responsibilities of the designated persons are as follows:

- The DP must ensure that requests for communications data are both necessary and proportionate prior to granting an authorisation or giving a Notice i.e. it should not be more than is required in circumstances, should not be arbitrary and should balance the extent of the intrusion or the interference of the individuals private life against a benefit to be achieved by the operation and the public interest
- The DP should not be responsible for granting authorisations or giving Notices in relation to investigations or operations in which they are directly involved (unless it is necessary to act urgently)
- The DP has a duty to consider various issues as follows:

I. Whether the case justifies the accessing of communications data under Section 22(2)(b) i.e. that it is for the prevention or detection of crime or preventing disorder;
II. Whether obtaining access to the data by the conduct authorised by the authorisation, or required off the CSP in the case of a Notice, is proportionate to what is sought to be achieved;
III. Whether the circumstances of the case still justifies such access in cases where there is likely to be collateral intrusion;
IV. Whether any urgent timescale is justified.

If an application is authorised, the DP should forward the completed form to the SPOC for further action. If an application is rejected, the DP should forward a copy of the rejected application to the SPOC with written reasons for the rejection. The original form should be forwarded to central records for monitoring and recording purposes.

Advice to assist the designated person when writing written considerations

1. It is fundamentally important that the DP must be able to evidence the fact that they have read and considered each application and based their considerations upon the principles of necessity and proportionality. It is a matter for the individual DP to decide how to demonstrate this effectively, bearing in mind that he or she could be called upon to justify the considerations at a later date in Court or at a Tribunal Hearing. It may well be appropriate in some cases to merely record the fact that the DP has read and considered the application and that he or she believes that obtaining the data in question is necessary and that obtaining the data by the conduct is proportionate to what is sought to be achieved by obtaining the data or words to that effect. This would largely depend upon the quality of the application and whether the DP is fully satisfied that the applicant has made out a strong case in all respects.

2. In practice the standard of applications will vary according to the knowledge and experience of the Applicant and therefore the DP will often be required to make a more detailed judgement. Equally it maybe that the application is quite complex or that it requests a particular in truth of set of data in which case the DP may wish to address this specifically. The DP's comments should be specific to the application in question

* ***For these reasons it is recommended that the DP should tailor the comments to the individual application as this is the best means of demonstrating that it has been properly considered.***

4. The Senior Responsible Officer (SRO)

The SRO is responsible for:

- Ensuring the integrity and lawfulness of the policy and processes within the Council
- Ensuring there is compliance with Chapter 11 of Part 1 of the Code of Practice
- Overseeing the reporting of errors to the interception of Communications Commissioner's Office
- Ensuring the implementation of any corrective action required for improving processes and minimising the likelihood of errors.
- Engaging with the ICCO Inspectors when inspections are carried out
- Where necessary oversee the implementation of post inspection action plans

The SRO is referred to in Appendix 1

5. The RIPA Officer

The RIPA Officer holds the following responsibilities:

- To retain a central record of all applications, authorisations and Notices
- To retain a record of the dates on which authorisations and Notices are started and cancelled
- To retain all applications in the event that they maybe a Complaints Tribunal
- To retain a record of any errors that may have occurred in the granting of authorisations, or issuing of Notices, and provide an explanation to the interception of Communications Commissioner

I. Procedural Guidance when making applications For communications data

Communications data maybe obtained by the Council giving a Notice under Section 22(4); or by granting an authorisation under Section 22(3).

Applications by Notice or Authorisations are valid for one month from when approval is given by the Designated Person. It maybe renewed at any time prior to the expiry of one month.

All applications should refer to a specific date or period. Where the date required is not specified, the relevant date taken will be the date that approval was granted for the application.

For the obtaining of communications data that will be generated in the future, disclosure may only be required of data obtained by the CSP within the month for which the application is valid. For historical communications data disclosure may only be required if in the possession of the CSP.

The designated person should give particular regard to the period of time that they are requesting data for and specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise would impact on the proportionality requirements and impose an unnecessary burden on CSP's.

The Act allows for 2 types of applications – application by notice or application for authorisation. Oral applications will be considered in limited situations.

1. **Notice under Section 22(4)**

A Notice is where a CSP collects and/or retrieves data in order to provide it to the Council. The form of Notice should be in writing. Oral notice is acceptable in urgent situations and is discussed in detail below. The Notice must include the following information:

- A description of the data required (and whether it is communications data under Section 22(4)(b) or Section 21(4)(c) of the Act);

- The purpose for which the data is required. **This will always be for the prevention or detection of crime or preventing disorder;**
- The name (or designation) and office, rank or position of the designated person;
- Record the date and time that approval was given by the DP;
- A manner in which data should be disclosed;
- A unique reference number;
- If relevant, any indication of urgency;
- A statement setting out that data is sought under the provisions of Part 1 Chapter 2 of the Act;
- Relevant SPOC details

The Notice must also be approved by the Designated Person before it can be served on the CSP. Once approval is given, the SPOC will serve the Notice to the CSP. When the data requested is provided, the SPOC will then feed it back to the Applicant and Designated Person.

2. Authorisation under Section 22(3)

An authorisation maybe used by the Council when the Applicant personally extracts/ collects or retrieves the communication data from the CSP.

This application may only be used when:

- the CSP cannot provide the communications data;
- It is believed that the investigation maybe prejudiced if the CSP is asked to provide the data;
- There is prior agreement in place between the Council and the CSP as to the appropriate mechanisms for the disclosure of communications data.

Each application must be in writing and must include the following information:

- a description of the conduct that is authorised
- a description of the communications data required (identify whether it is communications data under Section 21(4)(b) or Section 21(4)(c) of the Act)
- identify the purpose for which the data is required. **This will always be for the prevention or detection of crime or preventing disorder.**
- The name (or designation) and office, rank or position of the designated person
- A unique reference number (check that this document refers to unique reference number whenever referring to the application)
- Record the date and time that the application was approved

A Designated Person may only authorise persons working in the same Local Authority to engage in specific conduct to obtain communications data. This will normally be the authority's SPOC. The application must be cancelled by the Designated Person as soon as they are no longer considered to be either necessary or proportionate.

3. ORAL APPLICATIONS

An application for communications data may only be made and approved orally on an urgent basis, where:

I. There is an immediate threat to life such that a person's life might be endangered if the normal application procedure is followed; and/or
II. There is an exceptionally urgent operational requirement, within 48 hours, for the communications data; and/or
III. A credible, immediate and time-sensitive threat to national security exists; and/or

Note that when following the oral application route, the Applicant is still required to consult with the DP and SPOC. Written Confirmation from the DP and SPOC must be obtained that the oral application meets one of the three grounds set out above. The SPOC and DP are required to keep detailed records of all conversations and discussions relating to such an application. Details of the unique registration number, date and time that approval was granted by the DP must be recorded. The SPOC shall be responsible for orally advising the CSP of these details,

In the case of an oral notice, written notice must be given to the CSP retrospectively within one working day of the oral notice being given by the SPOC. Failure to do so will constitute an error reportable to the Information Commissioner.

As soon as possible after the period of emergency:

- The Applicant must complete a retrospective application form which includes an explanation of why the urgent process was undertaken;
- The Designated Person or SPOC must collate all records related to the oral application and subsequent written retrospective application and provide same to central records.

4. Renewals and Cancellations

Authorisations and Notices are valid for one month from the date on which the authorisation is granted. It is therefore vital that the application once approved is served within this time. (Month here means a Calendar month example a month beginning on 7 June 2009 ends on 6 July 2009).

Renewal maybe appropriate where there is a continuing need to acquire data that will (or may) be generated in the future. Any valid Authorisation or Notice maybe renewed for a period of up to one month by the grant of a further Authorisation or the giving of a further Notice. The renewal takes effect on the expiry of the Authorisation or Notice it is renewing.

The Designated Person should:

- consider the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated;
- record the date and, when appropriate to do so, the time when the Authorisation or Notice is renewed;

- consider carefully the length of any renewal and ensure that the renewal is valid for the shortest possible period.

If at any time after granting an application the Designated Person forms the view that the authorisation (including a renewed authorisation) is no longer necessary or that it is no longer proportionate to the objective sought, s/he must withdraw the authorisation. In such cases, where appropriate, the CSP should be advised of the withdrawal.

Provision of data requested by a CSP **does not** automatically cancel a Notice. It is primarily the duty of the Designated Person to ensure that any application is timeously cancelled. Where such cancellation is not timeously undertaken, the SPOC may undertake such cancellation on behalf of the Designated Person.

If at any time after giving Notice to a CSP and before it has been acted upon, the Designated Person forms the view that it is no longer necessary for the CSP to comply with the Notice, or where it is no longer proportionate to the objective sought, s/he must cancel the application.

Where a cancellation has been undertaken by the SPOC, the Designated Person must confirm the decision of the SPOC in a manner that creates a record of the application having been cancelled, along with reasons for such a cancellation.

Notification to a CSP of the cancellation of a Notice can be undertaken by the Designated Person directly or on that persons behalf, by the SPOC.

J. DATA PROTECTION PRINCIPLES

Disclosure of Communications Data by the CSP will be made to the Single Point of Contact (SPOC) who must:

- assess whether the data provided by the CSP fulfils the requirements of the Notice;
- assess whether the data acquired through an authorisation matches the authorisation

Any communications data acquired under the provisions of RIPA, together with all copies, extract and summaries shall be retained and/or destroyed in line with the Council's Records Retention and Destruction Policy. In addition the requirements of the Data Protection Act 1998 and its Data Protection principles should be adhered to.

The CSP can inform the data subject of the Application Notice if they receive a Subject Access Request under Section 7 of the Data Protection Act. However, the CSP can also use Section 29 Exemption (for the prevention and detection of crime) to withhold this information if disclosure could prejudice the investigation. This should be determined in relation or in liaison with the Council's SPOC.

K. Record Keeping

All documents and correspondence relating to Communications Data must be retained in written or electronic format. Such series of documents and correspondence should be physically attached or cross referenced where they are associated to each other.

Original copies of all documents and correspondence will be held by the central records. Copies will also be held by the Applicant, SPOC and/or Designated Person for their record purposes. There will therefore be at least three copies of each application to be held for record purposes.

The central record will also record the date when each application is granted, renewed or cancelled. These records must be available for annual inspection by the Information Commissioner.

The RIPA Officer must also keep a record of the following items:

- The number of applications submitted to a designated person for a decision to grant an Authorisation or give a Notice.
- The number of applications submitted to a designated person for a decision to grant an Authorisation or give a Notice which was rejected after due consideration
- The number of Authorisations or Notices to acquire Communications Data covering:
    - Section 21 (4)(b) – information about the use of Communications services (subscriber data)
    - Section 21(4)(c) – information and communications service users (service use data)
    - Any combination of the above
    - The number of urgent cases processed
- Number of times applications were granted orally.

This must be sent by the RIPA Officer to the Information Commissioner annually within a period as determined by him.

L. COMPLAINTS AND ERROR REPORTING

This policy aims to provide practical and realistic guidance. It is therefore only realistic to provide guidance on what should be done in the unlikely event of an error occurring. Legally, an error can only occur after a Notice has been served or data acquisition initiated from an Authorisation or Notice.

Examples of errors which could be made include:

- The purpose was not for the prevention or detection of crime
- Human error in what data requested and from whom
- CSP provides data not requested
- Notice granted which is not possible for the CSP to comply with
- Excess data requested include data inextricably linked to other information not required
- Same information has already been obtained from another source
- Traffic data requested

Errors may be divided into reportable errors (where communications data is acquired or disclosed wrongly is reported to the Information Commissioner) and recordable errors (where an error has occurred but is identified by the Council or CSP prior to the communications data being acquired or disclosed). Recordable errors are not reported to the Information Commissioner. However, details of such errors need to retained for inspection by the Commissioner.

Examples of Recordable Errors include

- a notice given which is impossible for the CSP to comply with;
- a failure to review information already held resulting in an application to acquire communications data or renew an existing authority in order to obtain information already acquired;
- The failure to serve written notice within 1 day of an oral application being granted.

Examples of Reportable Errors include

- An application for traffic data;
- Human error such as providing CSP with incorrect dates;
- Disclosure of the wrong data by a CSP when complying with a notice;

If an error is identified the relevant SPOC should complete the relevant form as a record of the error which includes:

- Details of the error
- Explanation of how the error occurred
- Indication of whether any unintended collateral intrusion has taken place and
- Indications of what steps have been or will be taken to ensure that a similar error does not occur

The completed form should be saved to the central monitoring record and the Senior Responsible Officer informed.

M. COMPLAINTS

Complaints about improper acquisition and disclosure of communication data maybe reported to the Interception of Communications Commissioner who may then report the case to the Investigatory Powers Tribunal or they may be reported directly by an effected individual to the Tribunal at Investigatory Powers Tribunal, PO Box 33220, London SW1H 9ZQ Tel No: 0207 035 3711.

Enquiries in the first instance maybe made to the Senior Reporting Officer at: The Borough Solicitor, London Borough of Hillingdon, Legal Services 3E/04, Civic Centre, High Street, Uxbridge, Middlesex UB8 1UW

N. SOURCES OF INFORMATION

1. Regulation of Investigatory Powers Act 2000
2. Statutory Instrument Order 2003 No 3172 (Powers of Public Bodies)
3. Home Office Code of Practice on the Acquisition and Disclosure of Communications Data (Draft 10/3/05)
4. Home Office Code of Practice on Interception of Communications

5. Home Office (http://security.homeoffice.gov.uk/ripa/)
6. Department of constitutional affairs guidance on the Data Protection Act (http://www.lcd.gov.uk/foi/datprot.htm)
7. Information Commission's Office (http://www.informationcommissioner.gov.uk)

O. APPENDICES

A – List of Officers with Designated Roles at the Council

Appendix A

List of Authorising Officers and authorising levels

Name	Area	Contact Number	Level of Surveillance Authority			
			Subsriber Data	Service Use Data	Oral	
Senior Responsible Officer						
Rajesh Alagh	Borough Solicitor	Ext 0617	Yes	Yes	Yes	
Designated Person						
Kathryn Sparks	Environment and Consumer Protection	Ext 7501	Yes	Yes	Yes	
Glen Egan	Legal Services Practice Manager	Ext 7602	Yes	Yes	Yes	
Single Point of Contact (SPoC)						
Sue Pollitt	Environment and Consumer Protection	Ext 7425	Yes	Yes	Yes	Home Office Accredited
Christopher Norris	Adult Social Care Health and Housing	Ext 0889	Yes	Yes	Yes	Home Office Accredited
Bill Hickson	Environment and Consumer Protection	Ext 7402	Yes	Yes	Yes	Home Office Accredited
RIPA Officer						
Beejal Soni	Licensing Lawyer	Ext 6425	No	No	No	