



ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

**REGULATION OF INVESTIGATORY POWERS ACT 2000
POLICY AND GUIDANCE NOTES**

Updated February 2009
Subject to Cabinet Approval May 2009

DRAFT

ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD
COVERT SURVEILLANCE POLICY AND PROCEDURAL GUIDANCE
(REGULATION OF INVESTIGATORY POWERS ACT 2000)

CONTENTS

Section	Page
Contents	ii
List of Annexes	iv
Why is RIPA Important?	v
1. Introduction	1
2. Definitions of Surveillance	3
3. Directed Surveillance	5
4. Covert Human Intelligence Sources	9
5. Compliance with this Policy	13
6. Relevant Legislation	14
7. General Rules on Authorisations	17
7.1 Need for Authorisation	17
7.2 Authorisation	17
7.3 Necessity	17
7.4 Proportionality	17
7.5 Collateral Intrusion	18
7.6 Who Can Grant Authorisation	19
7.7 Training of Authorising Officers & Officers Undertaking Surveillance	20
7.8 The Process of Obtaining an Authorisation	20
7.9 Emergency Authorisations / Unforeseen Circumstances	20
7.10 Backdated Authorisations	21
7.11 Information to be Provided in Applications for Authorisation	22
7.12 Duration of Authorisations	23
7.13 Review of Authorisations	23
7.14 Renewal of Authorisations	24
7.15 Cancellation of Authorisations	25
7.16 Recording of Authorisations / Reviews / Renewals / Cancellations	26
7.17 Consideration of Confidential Information	28
8. Use of Covert Surveillance Equipment	29
9. CCTV	31

Section		Page
10.	Guidance on Completing the RIPA Forms	32
11.	Reporting the Results of a Covert Operation	33
12.	Interception of Communications	34
13.	Examples of Actions that Local Authority Officers Cannot Undertake	37
14.	Codes of Practice	38
	- Home Office Code of Practice on Directed Surveillance	
	- Home Office Code of Practice on CHIS	
15.	The “Policing” of RIPA	39
16.	Consequences of Non Compliance	40
17.	Complaints Procedures	41
18.	Further Information	42

CONTENTS

LIST OF ANNEXES

Annex

1	Council's Authorising Officers for Covert Surveillance	44
2	R v Johnson Guidance	45
3	Special Arrangements for Authorising Surveillance where Confidential Material may be Involved	46
4	Notes of Guidance for Authorisation Tests – Directed Surveillance	47
5	Determination of Whether Directed Surveillance Authorisation is Required	51
6	Determination of Whether CHIS Authorisation is Required	52
7	Notes for Guidance on the Role of the RIPA Co-ordinator and Storage of Authorisation Forms	53
8	The RIPA1 Form – Guidance Notes for Completion	55

Why is RIPA Important?

Privacy is a right, but in any democratic society, it is not an absolute right. This is explicit in the European Convention of Human Rights, which permits intervention with an individual's privacy, where it is in accordance with the law, only if it is necessary for various specified reasons, including the prevention and detection of crime.

The right to a private and family life, as set out in the European Convention on Human Rights, must be balanced with the right of other citizens to live safely and freely : the most basic function that every citizen looks to the state to perform.

For these reasons the Regulation of Investigatory Powers Act 2000 and the Data Protection Act 1998 are important : they ensure that surveillance and the use of communications data are properly controlled and regulated, with independent oversight and a proper complaints procedure.

Royal Borough of Windsor and Maidenhead

REGULATION OF INVESTIGATORY POWERS ACT 2000 COVERT SURVEILLANCE POLICY AND PROCEDURAL GUIDANCE

1. Introduction

- 1.1 The Royal Borough of Windsor and Maidenhead's officers may at times, in the course of their investigatory, regulatory and enforcement duties, need to make observations of persons in a covert manner (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place) or to use a Covert Human Intelligence Source (CHIS), whether the subject of the investigation is a member of the public, an employee, owner of a business or a Council employee.
- 1.2 By its very nature, this sort of action is potentially intrusive and so it is extremely important that there is a very strict control on what is appropriate and that, where such action is needed, it is properly regulated in order to comply with Legislation and to protect the individual's rights of privacy.
- 1.3 RIPA is available to local authorities and may be used whenever appropriate for relevant activities carried out by either direct employees or contractors.
- 1.4 **It is the policy of this authority that, in so far as the Regulation of Investigatory Powers Act (RIPA) allows, surveillance and the use of CHIS will always be subject to the RIPA application process.** (See also para 1.9)
- 1.5 The only persons permitted by this Authority to authorise surveillance or the use of Covert Human Intelligence Sources (Authorising Officers), are those persons named in Annex 1 of this Policy.
- 1.6 The person responsible for monitoring the use of RIPA within this Authority (the "RIPA Monitoring Officer" or RMO) is the Head of Audit and Review. Any questions or observations about the use of RIPA or this Policy should, in the first instance, be addressed to them.
- 1.7 The objective of this document is to clarify the circumstances in which Council Officers will be permitted to carry out a Covert Surveillance operation and the requirements that will need to be observed in order that the Council will neither contravene the Legislation or the National Codes of Practice issued by the Home Office, the Information Commissioner's Office (formerly the Data Protection Registrar) and the Office of Surveillance Commissioners. Obtaining appropriate authorisation for surveillance will be of importance to ensure that any evidence obtained is not judged as being inadmissible in any subsequent legal proceedings, as well as providing the Council with some protection if the surveillance activities of its officers are ever challenged under the Human Rights Act, as part of a Judicial Review of a Council decision or in any reference to the Ombudsman.

- 1.8 This Policy and Guidance, operational from 28 May 2009 (after formal Cabinet approval), updates and replaces the previous policy and guidance and will be reviewed regularly. 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 Guidance are to be observed by any contractor operating on behalf of the Council). Changes to the policy will always be subject to the approval of the Cabinet, except insofar as changes are made to the appendices to reflect changes in personnel or alterations to the Home Office approved RIPA forms.
- 1.9 It is the policy of this authority that, where officers wish to undertake activities that may involve a breach of a person's right to privacy but which do not fall within the scope of RIPA, a similar process of considering the proportionality and necessity of any such activities must be carried out before the activities are undertaken, and approval gained from a RIPA authorising officer. The RIPA Monitoring Officer and Head of Legal Services are available for advice if required.
- 1.10 Note : Within the Policy, definitions appear in grey boxes, examples within blue boxes.

2. Definitions of Surveillance

2.1. Covert Surveillance

- 2.1.1. RIPA defines covert surveillance and then differentiates between *directed* and *intrusive* surveillance.

Covert Surveillance is surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. Covert Surveillance can be either **Directed Surveillance** or **Intrusive Surveillance**.

2.2. Directed Surveillance

Directed Surveillance is surveillance which is covert but not intrusive and which 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 specifically identified for the purposes of the investigation or operation; and
- c) not in immediate response to events or circumstances, which would make prior authorisation unreasonably practicable.

- 2.2.1. Examples of surveillance that would be classified as being Directed Surveillance are detailed in the table at paragraph 3.1.

- 2.2.2. Directed surveillance does not include covert surveillance carried out as an immediate response to events or circumstances, which by their nature could not have been foreseen, e.g. a Police Officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

2.3. Intrusive Surveillance

- 2.3.1. Intrusive surveillance is the term used to cover carrying out surveillance by going on to, or placing a device into private dwellings to gather information about the occupier(s).

Intrusive surveillance is defined in Section 26(3) of RIPA as Covert Surveillance that:

- a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

- 2.3.2. Local Authorities are **NOT** authorised to conduct Intrusive Surveillance without the consent of the Secretary of State.

2.4. Included Within Surveillance

- 2.4.1. **Surveillance**, according to RIPA, includes most acts of observing someone in a covert way.

Section 48 (2) of the act says that these activities are surveillance :

- A:** "Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications. (In S81, communication is defined as anything comprising speech, music, sounds, visual images or data of any description, and signals serving either for the impartation of anything between persons, a person and a thing or between things on actuation or for the control of any apparatus);
- B:** Recording anything monitored, observed or listened to in the course of surveillance; and
- C:** Surveillance by or with the assistance of a surveillance device.

- 2.4.2. Surveillance can **also** include the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication (refer to Section 12).

2.5. Private Property

- 2.5.1. On occasions, employees may wish to carry out covert surveillance involving private property. **This must only be done in serious cases where no reasonable alternative exists.**
- 2.5.2. Note that surveillance involving the presence of an officer or a device on the same private property as the subject is *intrusive* and falls under paragraph 2.3 *et seq.*
- 2.5.3. Where officers intend to use private residential property as an observation point, they must refer to the guidance in R v Johnson (Annex 2).
- 2.5.4. Due to the importance of justifying any intrusion under Article 8 of the HRA, this must not be done without legal advice.

2.6. Changes and Areas of Doubt

- 2.6.1. This is a developing area. It is not always easy to recognise what comes within or without RIPA. The examples in blue boxes, throughout this Policy, provide some examples of what is and what is not included.
- 2.6.2. **Where there is doubt as to whether this Policy and Guidance applies to an area of operation, the officer must seek the advice of the Head of Audit and Review or the Council's Legal Services Section prior to any action being taken.**

3. Directed Surveillance

- 3.1. The table below gives some examples of the types of work where Directed Surveillance may be required in order to fulfil the Authority's investigatory, regulatory and enforcement functions.

Examples of Directed Surveillance:

Resources Directorate

- Undertaking investigations into allegations of internal fraud may require surveillance activity.
- Covert observation of benefit claimants to ascertain whether or not they are committing benefit fraud by, for example, working or living as a couple.

Childrens' Directorate

- Complying with Child Employment law and the protection of young or vulnerable persons may lead Education and Social Services staff to check whether children are working beyond legally authorised limits.
- School inspectors determining truancy from school and possible prosecution of parents / guardians by carrying out covert observations. (N.B: Observations involving children must be treated with exceptional care.)

Environment Directorate

- Covertly observing property where there is a reason to believe that a landlord may be committing offences related to overcrowding, but not openly undertaking housing visits to check occupancy levels of a premises for overcrowding.
- Covertly recording nuisance behaviour by tenants (whether by Housing Officers or contractors engaged by them) but not the recording of noise nuisance by normal recording devices.
- Enforcing controls on minerals and waste activities in relation to illegal activities that may be part of planning enforcement investigations.

All Directorates

- Compliance with anti discrimination legislation and the Council's Human Resources Policies, e.g. Diversity and Equality.

CCTV and Business Watch

- Using a town centre CCTV to track an individual in a planned operation that the individual is unaware of.

The above list is not exhaustive but is illustrative of the types of activities that local authority investigators engage in and which would be classified as "Directed Surveillance" (see Section 2 for Definitions).

- 3.2. There are many occasions where we watch people in a way that is NOT directed surveillance, either because the watching is done openly, or because the covert nature is incidental to other work we are doing.
- 3.3. The table below gives some examples of the types of operation that are NOT Directed Surveillance.

Examples of what is not Directed Surveillance:

- “Hot spot targeting”, e.g. licensing officers standing on a street to monitor private hire cars plying for hire illegally where this is not part of a planned operation, or surveillance on fly tipping and dog fouling clear up. (Home Office Guidance refers.)
- Test purchases for sale of alcohol to under 18s.
- CCTV cameras (unless they have been directed at the request of investigators) – these are overt or incidental surveillance, and are regulated by the Data Protection Act.
- Activity that is observed as part of normal duties, e.g. by an officer in the course of day-to-day work. (Excluded by RIPA.)
- Overt investigations, such as :
 - Benefits Officers visiting a person to make enquiries and declaring their status and intention ;
 - Environmental Health Officers declaring their status and intention; and
 - Monitoring for Human Resources reasons of which the employee has been made aware.

3.4. Information Received from Members of the Public acting on their own Volition

- 3.4.1. RIPA does not apply to information volunteered by members of the public acting on their own volition (e.g. neighbours filming next door's nuisance activities from across the road and then giving the tape to Environmental Health), unless they have been actively recruited to do so, or have been asked to continue what started as a voluntary act. Such information is normally available as evidence, subject to the normal admissibility rules, such as PACE S.78. (In general terms, such evidence will be admissible so long as its probative value outweighs any prejudice against the accused).
- 3.4.2. Where information is offered by members of the public, it must be carefully graded, using the National Intelligence Model '5x5x5' system. Great care must be taken when deciding to use or disseminate intelligence or evidence gained from a member of the public, and consideration should be given to both the immediate risk to the source and to their continued (longer term) safety. The prolonged use of a person, who regularly provides information to the authority, may constitute the creation of a Covert Human Intelligence Source (see section 4).
- 3.4.3. When Council officers decide to use someone complaining of statutory nuisance to gather evidence to substantiate the

complainant's claims (e.g. by using digital equipment to record noise nuisance); they are required to use the Environmental Health Team procedures. Following the relevant procedures will ensure that any evidence gathered will be done in an overt manner and will not, therefore, fall within the scope of RIPA. **Reference must be made to the Environmental Health Unit in such instances. Consideration of the source's safety must still be considered as in 3.4.2 (above).**

3.5. Internal Application of RIPA

3.5.1. **RIPA is NOT available to authorise monitoring of behaviour that falls short of criminal activity. Under those circumstances, see paragraph 1.7 (above).**

3.5.2. RIPA can have an internal focus if, and only if, criminal activity is being investigated. Directed Surveillance may be authorised if officers are conducting criminal investigations of employees in the context of employment relationships. This does not include investigations into sickness absence that is suspected as not being genuine or misconduct in the workplace, unless they have reached the level of being a criminal investigation. More details are set out in the Council's relevant employment policies, namely the Management of Sickness Absence Policy and Disciplinary Procedure, which are available on the Council's Intranet or from the Human Resources Unit, on request.

3.5.3. Regular monitoring, where it is to be expected that this will be carried out in the normal course of the running of the Council's business, would be regarded as falling outside RIPA. This is because there would be implied consent for such monitoring for various reasons, including dealing with matters in an employee's absence for holiday, illness or other reason.

3.5.4. Monitoring :

- to ensure that equipment is being used in accordance with Council policies
- internal Email systems or information stored on a server
- telephone calls
- internal and external post (unless clearly identified as private and personal and not expected to be opened in an employee's absence)
- times of entry and exit may take place, using the staff identification card system

is NOT covered by RIPA as it is normal employment practice, provided all reasonable efforts have been made to inform all potential users that monitoring may be undertaken. (e.g. inclusion in Council Policies and Procedures issued to all staff, notification on Email / Intranet).

3.5.5. **Note: It must be made clear to all employees that staff identification cards create a computer history, which may be used for monitoring purposes, that emails may be monitored, that routine checks of computer use may be carried out and that these are a condition of employment with the authority.**

- 3.5.6. **NB: It is emphasised that use of RIPA for monitoring an officer's use of internal Email and the internet and other such monitoring can only be authorised when properly judged to be necessary on one of the specified grounds for authorisation (refer to section 7).**

4. Covert Human Intelligence Sources

4.1 This is the second way that local authorities are directly affected by RIPA.

A person is a **Covert Human Intelligence Source (CHIS)**, if -

- A** they establish or maintain a personal or other relationship (this must be a relationship and not a conversation) with a person for the covert purpose of facilitating the doing of anything in **B** or **C**.
- B** covertly using the relationship to obtain information or provide access to any information about another person or,
- C** covertly disclosing information obtained by the use of such relationship, or as a result of its existence.

4.2 A CHIS can be created by inducing, asking or assisting a person to engage in the conduct of a source or obtaining information by using that source. **Note the word 'induced'. If you imply to a member of the public that you would like them to carry out CHIS activities, even if that is not your intention, you may accidentally create an unauthorised CHIS.**

A purpose is covert ONLY if it is conducted in a way calculated to ensure that one party is unaware of the purpose.

Information or intelligence is used covertly if one party was unaware of the use or disclosure of information obtained.

- 4.3 There are many situations in which a person may be regarded as a CHIS. The following tables give some guidance :-

When is a person a CHIS?

Examples of a CHIS may include:

- Licensing officers, working with the Police, covertly building a business relationship with a cab company which is believed to be using unlicensed drivers.
- Whistleblowing, when you actively "recruit" an employee to gather information on another employee who is the subject of a criminal investigation, provided this is undertaken within a formal framework (refer to the Council's Raising Concerns at Work (Whistleblowing) Policy).
- Food safety officers posing as customers to get information on what is being sold at a premises and developing a relationship with the shopkeeper beyond that of supplier and customer.

When is a person NOT a CHIS?

A CHIS would not be:

- A member of the public who volunteers information to the local authority, such as a person who complains that they purchased food past its 'use by date' from their local supermarket. In that case the relationship between customer and provider is too remote. If the information were to be provided by an employee of the supermarket who was alleging that the food was being sold past its 'use by date', then such a person is likely to be a CHIS as a relationship exists, namely one of employer / employee, and they are covertly disclosing information they have obtained as a result of that relationship.
- An officer who merely goes into a shop and purchases an item without engaging in dialogue except for 'how much'? and 'thank you', would not be a CHIS as, although the officer is working under cover, the officer is not seeking to build a relationship with that person or to gain that person's trust.
- An officer who attends premises and identifies him / herself and then either carries out a statutory inspection or has entered in pursuance of a warrant of entry issued by a court, is not a CHIS. There is nothing covert about their visit.
- Council officers being invited to use a resident's property to undertake surveillance to obtain evidence in respect of a neighbour to assist a benefit fraud investigation. **This is directed surveillance. Refer to the rules of *R v Johnson* (Annex 2) for guidance on the use of private premises.**

Management of a CHIS

- 4.4 An Authorised Officer may not grant an authorisation for use of a CHIS unless they are satisfied that the following persons and processes are in place.
- 4.5 At all times there will be an officer who will have day to day responsibility for dealing with the source on behalf of the Council and for the source's security and welfare (the 'Tasking Officer').
- 4.6 The Tasking Officer will be the person who:
 - 4.6.1 contacts and deals with the source on behalf of the council;
 - 4.6.2 directs the day to day activities of the source;
 - 4.6.3 makes a permanent record of the information provided by the source (with reference to rules of Data Protection and CPIA); and
 - 4.6.4 monitors the security and welfare of the source.
- 4.7 At all times there will be another officer, senior to the Tasking Officer, who will have general oversight of the use made of the source (the 'Supervising Officer').
- 4.8 The RIPA Monitoring Officer will maintain a record of sources used, and allocate a reference number for each source. Information from that source will never bear the source's name, but will, instead, bear the reference number. There are legal procedures in place that protect the identity of sources, and this authority will always seek to use these.
- 4.9 The Council will not reveal the identity of a source to any person outside the handling and authorisation process, unless required to do so by a Judge. If the circumstances of an investigation mean that disclosure of a source's identity is likely to be required, this will be discussed with the source by the Tasking Officer **before** any use is made of the source.
- 4.10 Information obtained from a source must always be considered as sensitive and stored securely and used with especial care. It is likely to be allocated a handling code 4 or 5 under the National Intelligence Model and, if unused, marked as 'sensitive unused material', for the purposes of the Criminal Procedures and Investigations Act 1996.

Safety and Welfare of a CHIS

- 4.11 The safety and welfare of the source and foreseeable consequences to others must be taken into account in deciding whether or not to grant an authorisation. A risk assessment must be carried out determining the risk to the source in acting as a source of information to the Council and in particular, identifying and assessing the risks should the identity of the source become known. The welfare and security of the source after operations have ceased must be considered at the outset. The Tasking Officer must report to the Supervising Officer any concerns about the personal circumstances of the source, insofar as they might affect:
 - 4.11.1 the validity of the risk assessment
 - 4.11.2 the conduct of the source, and

- 4.11.3 the safety and welfare of the source.
- 4.12 The Tasking Officer may also be a CHIS and their health and safety must not be overlooked. If officers are to be used as a CHIS, the arrangements mentioned above must be followed so that the source is correctly managed.
- 4.13 The use of vulnerable individuals, such as the mentally impaired, for a CHIS purpose may only be authorised in the most exceptional cases. Authorising Officers must also abide by the Home Office Code of Conduct relating to Juveniles. **Vulnerable individuals must not be used as a CHIS, except in accordance with the Home Office Code of Practice and then only if authorised by the Head of Paid Service.**
- 4.14 If appropriate, such concerns must be reported to the Authorised Officer who will need to determine whether or not to allow the authorisation to continue.

5. Compliance With This Policy

- 5.1 Whether you are an applicant, an Authorising Officer or involved in investigations or monitoring of RIPA in any other way, in order to avoid any issues of non-compliance, you must ensure that:
 - 5.1.1 surveillance is carried out in accordance with the relevant Legislation ([Section 6](#)).
 - 5.1.2 proper authorisations are obtained ([Section 7](#)).
 - 5.1.3 when authorisation forms are completed, they are correct ([Section 7](#)).
 - 5.1.4 proper consideration is given to ensuring that surveillance is necessary and proportionate ([Section 7](#)).
 - 5.1.5 authorisations are properly recorded and monitored ([Section 7](#)).
- 5.2 The remainder of this document provides guidance as to how the above can be achieved. Notes for guidance and flowcharts to assist in determining whether authorisation is required are detailed at Annexes 4 to 8.
- 5.3 This Policy and Procedural Guidance has been developed by the Head of Audit and Review, Audit and Review Unit, in consultation with Senior Management Team, Legal Services, the Data Protection Officer, the Council's Section 151 Officer, officers from the Environment Directorate and other relevant officers from the Council. Any enquiries about this Policy must be referred to the Head of Audit and Review, who is also designated as the Council's RIPA Monitoring Officer.

6 Relevant Legislation

6.1 Regulation of Investigatory Powers Act 2000 ("RIPA")

6.1.1 RIPA provides a process by which public bodies can demonstrate that their surveillance and use of CHIS are lawful and comply with privacy legislation. It also provides for the regulation of covert surveillance for a number of public bodies, including local authorities. It is a tool to help officers demonstrate the correct balance between an individual's rights to privacy, and the proper use of data and surveillance as part of evidence gathering.

6.1.2 RIPA brought together various rules on the gathering of covert evidence, helped to standardise various legislation on lawful interception and surveillance, and takes account of the advances in technology, such as the Internet.

6.1.3 It is important to note that, whilst covert surveillance is used in many of the jobs we do (such as nuisance information gathering, and regulating the workplace), RIPA is only available to Local Authorities when they are investigating Criminal Acts.

6.1.4 Although RIPA is available to Local Authorities, and they are strongly advised to use RIPA to authorise directed surveillance and CHIS where appropriate, covert surveillance and the use of CHIS by a public body would not be unlawful merely because it was not authorised in accordance with RIPA.

6.1.4.1 The main advantage of following RIPA is to show that directed surveillance and the use of a CHIS has been carried out in a lawful manner.

6.1.4.2 If RIPA is not followed, the corollary is not true; i.e. it does not make conduct carried out under it unlawful. However, it provides a useful audit trail and focuses the mind to the Human Rights Act 1998 which may have to be justified in other ways if the RIPA framework is not followed.

6.1.4.3 Where RIPA is not available to a Local Authority, similar considerations still apply to any potential breach to a person's right to privacy.

6.1.4.4 This Authority instructs all staff that covert operations may only be carried out if approved by an appropriate RIPA Authorising Officer.

6.2 The Data Protection Act 1998 ("DPA")

6.2.1 The DPA provides eight principles to be observed to ensure that the requirements of the Act are complied with. They provide that personal data, which includes personal data obtained from covert surveillance techniques, must:-

- be fairly and lawfully obtained and processed;
- be processed for specified purposes and not in any manner incompatible with those purposes;

- be adequate, relevant and not excessive;
- be accurate;
- not be kept for longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure;
- not be transferred to non-European Economic Area Countries without adequate protection.

6.2.2 Sections 29, 34 and 35 of the DPA contain the exceptions to normal data handling principles.

6.2.3 **Personal information gathered as part of criminal investigation is never disclosable under s.7.**

6.2.4 More information on data protection issues is available from the Information Commissioner's website at <http://www.ico.gov.uk/> and on the Council's Intranet under Corporate Area / Information Management / Legal Related Information Management Policies.

6.3 Freedom of Information Act 2000 (FOIA)

6.3.1 The FOIA provides for the general rights of access to recorded information held by public authorities and specifies the conditions before a request has to be complied with. RIPA authorisation documents do not fall within the scope of the FOIA as they contain personal information and are subject to DPA.

6.3.2 Information that, if disclosed, may prejudice the outcome of a future investigation must not be disclosed as part of a FOIA disclosure. This covers most documentation relating to authorisations for directed surveillance.

6.3.3 If in doubt, officers should seek the advice of the Head of Legal Services.

6.4 The Human Rights Act 1998

6.4.1 This came into force on the 2nd October 2000 and enabled an individual to enforce rights and freedoms guaranteed under the European Convention on Human Rights through the domestic Courts in relation to acts of a public body. The most important articles in the context of RIPA are Article 8 (the right to respect for private and family life, home and correspondence), and Article 6 (the right to a fair trial). Article 6 includes internal procedures for hearings and fairness extends to the way in which evidence is obtained.

6.4.2 Evidence therefore, needs to be gathered in such a way that the interference with those rights is clearly justified and reasonable. This is because there must be no interference with Article 8 rights by a public authority except where interference is in accordance with the law, is necessary in a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others.

6.5 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 S.I. 2000/2699

6.5.1 These Regulations permit the Council to, without further authorisation, lawfully intercept its employees' E-mail or telephone communications and monitor their Internet access for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems, as long as these are applied proportionately and with safeguards for the protection of personal freedom.

6.6 Home Office Codes of Practice on Using Covert Surveillance and Covert Human Intelligence Sources

6.6.1 When carrying out such surveillance or using CHIS, officers must also bear in mind the Codes of Practice on using Covert Surveillance and Covert Human Intelligence Sources, issued by the Home Office.
<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/>

7 General Rules on Authorisations

7.1 Need for Authorisation

7.1.1 Obtaining appropriate authorisation for directed surveillance will be of importance to ensure that any evidence obtained is not to be judged inadmissible in any subsequent legal proceedings, as well as to provide the Council with some protection if the surveillance activities of its officers are ever challenged under the Human Rights Act, as part of a Judicial Review of a Council decision or in any referral to the Ombudsman.

7.1.2 The only ground available to a Local Authority for the use of RIPA is for the purpose of preventing or detecting crime. Whenever it is proposed to conduct Directed Surveillance or to use a CHIS, an authorisation must be sought under Part II of the Regulation of Investigatory Powers Act 2000, as set out in the following paragraphs.

7.2 Authorisation

7.2.1 An authorisation *may not* be granted unless the Covert Surveillance / use of CHIS have satisfied two criteria. It must be both: -

Necessary and Proportionate

7.3 Necessity

7.3.1 The Covert Surveillance / use of CHIS must be considered to be necessary for the purpose of preventing or detecting crime or of preventing disorder.

7.3.2 The evidence it is proposed to obtain by covert means must be necessary to prove a part or parts of the offence under investigation.

7.3.3 It must be clearly demonstrated, through the application, that the surveillance is likely to obtain evidence of significant probative value, i.e.: without the evidence the outcome of the investigation is likely to be prejudiced. Surveillance that will provide a trivial contribution in evidence is unlikely to be necessary and should not be authorised unless clearly demonstrated otherwise.

7.3.4 **The application MUST make it clear how the proposed intrusion is necessary and how an absence of this evidence would have a prejudicial effect on the outcome of the investigation. If it does not, the application MUST be refused.**

7.4 Proportionality

7.4.1 Even if the proposed activity is considered to be necessary, the person considering the application for authorisation must consider whether 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 target and others who might be affected by it against the need for the activity. The consideration of proportionality should involve the following questions: -

- 7.4.1.1 How serious is the offence?
- 7.4.1.2 Are there any less intrusive ways that similar evidence may be obtained?
- 7.4.1.3 How great is the interference in the privacy of the subject?
- 7.4.1.4 How great is the interference in the privacy of any others with whom the subject may come into contact? (“Collateral Intrusion”)

7.4.2 The level of interference in a person’s private life must be justified by the seriousness of the offence. The CPS Code for Crown Prosecutors gives advice about what could be considered ‘aggravating features’ of an offence, such as: -

- 7.4.2.1 risk of high levels of loss if the offence is allowed to continue; and;
- 7.4.2.2 offences that are prevalent in the Authority’s area.
- 7.4.2.3 If there are **less intrusive** methods of investigation available that would be likely to obtain similarly probative evidence, surveillance will not be necessary unless:
 - 7.4.2.4 following those methods has already been tried and failed; or
 - 7.4.2.5 following those methods would pose a serious risk to the success of the operation.

7.4.3 The officer applying for authorisation to conduct surveillance must take into consideration the expected level of privacy that the subject of the surveillance will have during the proposed operation, seeking to reduce the intrusiveness where possible. This may include reducing: -

- 7.4.3.1 time periods
- 7.4.3.2 the use of recording devices
- 7.4.3.3 mobile surveillance to static surveillance
- 7.4.3.4 the duration
- 7.4.3.5 number and type of locations visited (e.g. residential, workplace)

7.5 Collateral Intrusion

Collateral intrusion means intrusion into the privacy of persons other than those who are the subject of the investigation.

7.5.1 Measures must be taken to minimise both the risk of such intrusion and the extent of such intrusion. An application for authorisation must consider the risk of such intrusion and the Authorised Officer must take such risk into account in reaching a judgement as to whether or not the proposed Directed Surveillance / use of a CHIS is **proportionate**.

7.5.2 Those carrying out the surveillance must inform the Authorised Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration must be given as to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

7.5.3 Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities, which could impact on the deployment of surveillance. Liaison with the Police is recommended, where appropriate.

7.5.4 The person applying for surveillance must show that any collateral intrusion that is likely to occur is unavoidable without jeopardising the effectiveness of the operation, and it is still proportionate to conduct surveillance even with the risk of collateral information being obtained. Collateral information obtained must be treated in accordance with CPIA and protected from inappropriate disclosure, in accordance with the National Intelligence Model.

Examples of cases in which surveillance will not be proportionate.

- A surveillance operation that investigates a 'one off' minor offence that has no real risk to public safety and a minimal loss to public funds.
- A non-serious case that involves watching and photographing a person who is working at a children's playground, when the photographs will include the children and their parents.
- Following a person home to confirm that they are still living in their council property, when you could obtain the same information by visiting them without prior notification.

7.6 Who Can Grant Authorisation?

7.6.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 SI2003 No. 3171 lists the Authorising Officers for a 'relevant authority'¹. This prescribes that in a local authority, authorisations for Directed Surveillance and the use of a CHIS may only be granted to Assistant Chief Officers, Assistant Head of Service, Service Manager or equivalent. These will be designated as "Authorising Officers". Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable in the case of small organisations or where it is necessary to act urgently. Where an Authorised Officer authorises such an investigation or operation, the central record of authorisations must highlight this and the attention of a Commissioner or Inspector must be invited to it during their next inspection.

7.6.2 As the Council does not have officers designated as Assistant Chief Officers, the Chief Executive has granted that authorisations may be given only by the officers designated in this code, who will be at Director or Head of Service level, as set out in Annex 1. These officers must not act as the "Authorising Officers" for Covert Surveillance if: -

7.6.2.1 The case and surveillance is to be carried out in their own unit;

7.6.2.2 For any reason they have a vested interest in the case.

¹ Relevant authority in England includes a County Council, District Council, London Borough Council, Common Council of the City of London in its capacity as a local authority, Council of the Isles of Scilly

7.6.3 This list will be maintained by the RIPA Monitoring Officer. Additions / deletions will be made with that officer's approval only.

7.6.4 Annex 3 of the RIPA Policy and Guidance Notes detail the special arrangements for authorising surveillance where confidential material may be involved.

7.7 Training of Authorising Officers and those Undertaking Surveillance

7.7.1 In accordance with this Code of Practice, Authorising Officers **must** receive full training in the use of their powers. They must be assessed at the end of the training, to ensure competence, and must undertake refresher training at least every two years. Training will be arranged by the Head of Audit and Review. Designated Authorising Officers who do not meet the required standard, or who exceed the training intervals, are prohibited from authorising applications until they have met the requirements of this paragraph. Authorising Officers must have an awareness of appropriate investigative techniques, Data Protection and Human Rights Legislation.

7.7.2 Those officers who actually carry out surveillance work must be adequately trained prior to any surveillance being undertaken. A Corporate training programme will be developed to ensure that Authorising Officers and staff undertaking relevant investigations are fully aware of the legislative framework.

7.7.3 **Authorising Officers will not be able to authorise surveillance activities until they have received appropriate training.**

7.8 The Process of Obtaining an Authorisation

7.8.1 All requests to **conduct, extend or discontinue** a Covert Surveillance exercise or use a CHIS must be made in writing on the appropriate forms, as specified by the Office of Surveillance Commissioners (see Application Forms and Guidance Notes Pack which accompanies this document) and be submitted to an appropriate Authorised Officer of the Council (Annex 1). Sufficient time must be given for the Authorised Officer to consider the application.

7.8.2 All requests must be considered and authorised in writing by an Authorised Officer before any Directed Surveillance operation can commence.

7.8.3 Both the officer seeking the authorisation and the Authorised Officer shall have regard to the factors detailed in section 7, in respect of granting authorisations.

7.9 Emergency Authorisations / Unforeseen Circumstances

7.9.1 When an officer acts in immediate response to events as they unfold, this would not be classified as Directed Surveillance requiring RIPA authorisation. **No authorisation need be sought for this situation such as an enforcement officer who, by chance, witnesses unlawful activity and follows the suspect to find out their address.**

7.9.2 Surveillance that has become systematic and no longer immediate in its response to events must be authorised by either an emergency oral authorisation or by discontinuing surveillance until a written authorisation can be sought.

7.9.3 Oral authorisation can be granted for a maximum of seventy-two hours in an emergency situation, that is where it is not practicable to complete a written application and surveillance must be carried out to prevent valuable evidence being lost. Oral authorisation must never be used as an alternative to written due to poor planning or organisation by an investigator.

If an officer wishes to obtain urgent oral authorisation for surveillance, he must telephone an Authorising Officer to provide the following information:

- Full details of the person to be subject of the surveillance;
- The offence being investigated, and its seriousness;
- How the investigation is necessary to the business of the Authority;
- How surveillance is necessary to the investigation;
- How surveillance is proportionate bearing in mind the offence, the expectation of privacy and the collateral intrusion; and
- What the impact of ceasing surveillance and obtaining a written authorisation would be.

7.9.4 As soon as possible following the Oral Authorisation, the written application for Authorisation must be completed. A case is not normally regarded as urgent unless the time that would elapse before the Authorised Officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need has been neglected or the urgency is of the Authorised Officer's own making.

7.10 Backdated Authorisations

7.10.1 Under **no** circumstance must any Covert Surveillance operation be given backdated authorisation after it has commenced. Embarking upon Directed Surveillance or the use of a CHIS without authorisation, or conducting Covert Surveillance outside the scope of the authorisation will not only mean that the 'protective umbrella' of RIPA is unavailable, but may result in disciplinary action being taken against the officer / officers concerned within the Council's Human Resources Policies and Procedures.

7.10.2 If any person becomes aware of unauthorised surveillance, or of attempts to backdate a surveillance operation, they must report this **immediately** to the RIPA Monitoring Officer.

7.11 Information to be provided in Applications for Authorisation

7.11.1 Written application for authorisation for Directed Surveillance must describe any conduct to be authorised and the purpose of the investigation or nature of any surveillance.

The application must also include:

- the reasons why the authorisation is **necessary** in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in paragraph 7.3;
- the reasons why the surveillance is considered **proportionate** to what it seeks to achieve, listed in paragraph 7.4;
- the nature of the surveillance, including a sketch map showing relevant location of area under surveillance and location of officer;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

Additionally, in **urgent** cases, the authorisation must record (as the case may be):

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

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

7.12 Duration of Authorisations

7.12.1 Authorisations have the following statutory durations (and, therefore, cease to have effect after):

- Directed Surveillance – three months
- Covert human intelligence source – twelve months
- Emergency authorisation – seventy-two hours only, unless renewed.

How to calculate the expiry of an authorisation:

An officer applies for permission to carry out surveillance, on a named subject, which is necessary to the proof of a case of serious fraud. The Authorising Officer considers that it is proportionate, and approves and signs the RIPA1 form at 3.35pm on 23rd March 2010.

Applications for *Directed Surveillance* last for three months.

The expiry is midnight on the final day of the authorisation: 22nd June 2010.

7.13 Review of Authorisations

7.13.1 Once granted, an authorisation must be reviewed regularly by the officer managing the case to assess whether or not the investigation continues to be necessary and proportionate. The Authorised Officer must be notified of any instances where these criteria are no longer met. Reviews must be more frequent when access to confidential information or collateral intrusion is involved. Review frequency will be as often as the Authorised Officer deems necessary, in the circumstances of the case.

7.13.2 When authorising covert activities, Authorising Officers must set, as a minimum, the first review date of a case. This must be no more than four weeks from the date of authorisation.

7.13.3 Where possible (and it is good practice so to do) Authorising Officers should set a programme of reviews at the time they first authorise the covert activities. This programme should be kept under review and amended as necessary.

7.13.4 The forms contained on the Council's Intranet must be used in conducting a review of Covert Surveillance or a CHIS.

7.13.5 The results of a review must be recorded on the central record of authorisations (paragraph 7.16.3). Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential material (refer Annex 3) or involves collateral intrusion (paras. 7.5.1 to 7.5.4).

7.14 Renewal of Authorisations

- 7.14.1 If at any time before an authorisation would cease to have effect, the Authorised Officer considers it necessary for the authorisation to continue for the purpose for which it was given, they 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.
- 7.14.2 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal must not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.
- 7.14.3 An application for renewal must be made to the officer who granted the original authorisation unless there is very good reason not to do so (e.g. because the original Authorised Officer is on annual leave / has left the Authority).
- 7.14.4 Applications for renewal must be made using the forms contained on the Council's Intranet.

Applications for renewal of an authorisation for Directed Surveillance must record:

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

- 7.14.5 Authorisations may be renewed more than once, if necessary.
- 7.14.6 The renewal must be kept / recorded as part of the central record of authorisations.

To renew or not

Cases that are likely to be renewed would include the following:

- Surveillance has shown that the case involves more people than originally suggested, and the surveillance operation is to be widened to gather evidence against them.
- The surveillance has gathered three-quarters of the evidence required but is still crucially short of what is needed for a successful prosecution. The reason for this is that the investigator's car broke down on the last occasion.

Cases that are unlikely to be renewed would include the following:

- The investigators have been watching the subject for the last three months and have not seen him commit the offence. They are, however, sure he's 'at it' and would like another three months to have a look.

7.15 Cancellation of Authorisations

- 7.15.1 The Authorised Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the investigation no longer meets the criteria upon which it was authorised. This must be undertaken following a recommendation from the officer managing the case, who will continually review the investigation against the criteria. Where the Authorised Officer is no longer available, this duty will fall on the person who has taken over the role of Authorised Officer or the person who is acting as Authorised Officer.
- 7.15.2 It is the duty of the lead investigator to monitor the product of the covert activities against the objective set out on the application. As soon as that objective is achieved, the authorised activities must cease and the Authorising Officer asked to cancel the authorisation.
- 7.15.3 As soon as a decision is taken to cease the operation, an instruction must be given to those involved to stop all Directed Surveillance / using the CHIS. A form recording the cancellation must be completed. The forms contained within the "Application Forms and Guidance Notes for Completion Pack" which accompanies this document must be used in conducting a review of Covert Surveillance or a CHIS. The date and time when such an instruction was given must be recorded in the central record of authorisations and the notification of cancellation, where relevant.
- 7.15.4 Investigators must note that the cancelling of an authorisation does not remove the duty of care they have towards CHIS or other witnesses, particularly vulnerable ones.

7.16 Recording Authorisations / Reviews / Renewals / Cancellations

- 7.16.1 The originals of forms authorising / reviewing / renewing / cancelling Directed Surveillance or use of a CHIS must be forwarded to the Head of Audit and Review, who shall retain all such forms for a period of not less than three years after the surveillance has been discontinued. Similarly, the relevant directorate shall retain a copy of such forms for at least three years after the surveillance has been discontinued.
- 7.16.2 All new authorisations will be reported to the Council's Head of Audit and Review for consideration as to whether they amount to new uses requiring registration under the Data Protection Act.
- 7.16.3 A centrally retrievable record of all authorisations will be held by the Head of Audit and Review and regularly updated whenever an authorisation is granted, 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 must be retained for a period of at least three years from the discontinuance of the surveillance. The record will be kept by means of a simple spreadsheet kept in a secure directory with a hard copy retained securely with the supporting RIPA forms.

Information required to be recorded:

- the type of authorisation;
- the date the authorisation was given;
- name and position of the Authorised Officer;
- the unique reference number (URN) of the investigation;
- the title of the investigation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and name / position of the Authorised Officer;
- whether the investigation or operation is likely to result in obtaining confidential information;
- the results of the review of the authorisation;
- the date the authorisation was cancelled; and
- the reasons for any request being denied.

- 7.16.4 The Lead Member for Finance and Resources Overview and Scrutiny Panel will be sent a six monthly report identifying the number of authorisations that have been issued in respect of which function, setting out the category of covert surveillance undertaken e.g. observation of home or work from a public highway. For Data Protection purposes, the name or any details of the individual under surveillance will not be identified.

- 7.16.5 The Head of Audit and Review will be responsible for monitoring authorisations, carrying out an annual review of applications, authorisations, refusals, extensions and cancellations and maintaining a centrally retrievable record of authorisations.
- 7.16.6 Relevant directorates must ensure that any data is processed in accordance with Data Protection Legislation.
- 7.16.7 In the case of use of CHIS, records must be maintained in such a way as to preserve the confidentiality of the source and the information provided by the source. Due to the complex nature of CHIS management, any officer asked to register a CHIS will seek urgent advice from the local Police intelligence officer. Under no circumstances will a CHIS's personal data be recorded on a public computer drive or left on view in the office. As a minimum standard, CHIS details will be retained in a sealed envelope, within a second sealed envelope, in a restricted access safe with nothing marked on the outside of the first envelope apart from the name of the Tasking Officer and a unique reference number, and nothing marked on the second envelope apart from the name of the tasking officer and the words, "CONFIDENTIAL – NOT TO BE OPENED BY ANYONE EXCEPT <NAME> OR THE RIPA MONITORING OFFICER". Both envelopes must be signed across the seal by Tasking Officer and RIPA Monitoring Officer.
- 7.16.8 For urgent authorisations granted orally, an E Mail must be sent to the RIPA Monitoring Officer as soon as possible but not more than twenty-four hours after any such authorisation being granted.

The following particulars must be given:

- the type of authorisation (i.e. whether Directed Surveillance or use of a CHIS);
- the date and time of authorisation;
- the name and grade of the Authorised Officer;
- the unique reference number of the investigation and its title;
- a brief description of the investigation and names of subjects;
- whether the investigation is likely to result in obtaining "confidential information" (i.e. communications subject to legal privilege, information relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead who can be identified from it) or confidential journalism material); and
- the date the authorisation was cancelled.

7.17 Consideration of Confidential Information

- 7.17.1 The only person who may authorise surveillance involving confidential information is the Chief Executive (the 'Head of Paid Service') or, in his absence, a Chief Officer.
- 7.17.2 Because of the higher degree of expectation of privilege involved in Confidential Information, extra care must be taken. This may include the proportionality of the operation, the consideration of more regular reviews and the handling of the product of such surveillance. (Using the National Intelligence Model – 5x5x5 system, an information dissemination (handling) code of 4 would be normal in such cases).
- 7.17.3 'Confidential information' is defined within the Code of Practice as:
- information subject to legal privilege
 - personal information which includes
 - religious information held in confidence
 - confidential medical information
 - information relating to a confidential journalistic source
- 7.17.4 Matters subject to legal professional privilege, that is, oral or written communications and any items enclosed or referred to in them, between a professional legal adviser and a client that are to do with actual or contemplated court proceedings, are Confidential Information. Anything held with a view to furthering a criminal purpose is not subject to legal professional privilege and is not Confidential Information.
- 7.17.5 Confidential personal information is information held in confidence about a person (whether alive or dead), who can be identified from it and which relates to their physical health, mental health or spiritual counselling or other assistance given or about to be given, pursuant to a person's trade, business, profession, or other occupation or office (e.g. priest, counsellor). Information is held in confidence if held subject to an implied or express promise to hold it in confidence or is subject to a restriction on disclosure or an obligation of secrecy in existing or future legislation.
- 7.17.6 Confidential journalistic material is also part of confidential information. This is material acquired or created for journalism, given in return for a promise to hold it in confidence.

8 Use of Covert Surveillance Equipment

- 8.1 The use of recording devices in private residential premises, after the subject of the recording (normally a nuisance neighbour) has been told they will be monitored by the use of such devices, is not surveillance, it is monitoring. (Officers must, however, be aware of the risk to health and safety of the person allowing you to use their premises.)
- 8.2 In the event that officers wish to do other than monitor noise by use of surveillance devices, they must seek urgent advice from the RCMO or Head of Legal Services. The rules under which covert surveillance equipment may be installed on private premises are complex, and RIPA may not authorise the Authority to act in this way.
- 8.3 Surveillance equipment will only be installed in residential premises if a member of the public has requested help or referred a complaint to the Council and such matters can only be investigated with the aid of Covert Surveillance techniques after all the issues referred to in Section 7 have been considered. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant. (See paragraph 13.2.)
- 8.4 The following table gives examples of where Covert Surveillance equipment might be used: -

Examples of Where Covert Surveillance Equipment Might be Used

- A contractor is suspected of stealing supplies. Officers gain authorisation to observe the supply depot and to photograph any persons entering or leaving and to video any loading or unloading that takes place, using a concealed video camera.
- A benefit claimant is suspected of working in a market. Officers gain authorisation to observe the market stall and to photograph the subject, if he engages in trading activity, using a concealed still camera.
- A person is suspected of mis-selling service to persons on the street. Officers gain authorisation to approach the man and record the conversation, using a concealed tape recorder.

- 8.5 Any request by a Council officer to a resident to keep a video / audio / written diary as part of a Covert evidence-gathering exercise will be regarded as a Covert Surveillance exercise conducted on behalf of the Council and must be authorised as outlined in Section 7.
- 8.6 Generally, information gained under this type of operation will be given a dissemination code of 4 or 5, that is access will generally only be allowed to limited and prescribed parties, including law enforcement agencies, and prosecution agencies, and would have special condition attached to its use.

- 8.7 All information captured using a surveillance device and stored within recording media used during directed surveillance or as part of the conduct of a source, whether used or unused material, must be recorded and retained and revealed to the prosecutor according to the Criminal Procedure and Investigations Act (CPIA).

9 CCTV

- 9.1 The Authority has used and employed CCTV cameras in the town centre areas, car parks and other areas within the Borough for several years. A staffed control room is located at Council owned premises within the Borough. The CCTV equipment can record all cameras simultaneously throughout every 24-hour period. Since its inception, the CCTV monitoring scheme has been subject to a Code of Practice. The Code applies to CCTV systems overtly in public places to reduce, detect and prevent crime. It takes account of the Data Protection Act 1998 and Human Rights Act 1998. It remains unchanged by this document when used for overt surveillance. Reference must be made to the Council's "Code of Practice on CCTV", available on the Council's Intranet.
- 9.2 Covert surveillance can also be by way of hidden cameras in a public place or by targeted CCTV, that is where a CCTV camera is trained on a specific person or a spot at a particular time in order to observe the activities of a particular person or group of persons, in which case it would require authorisation in accordance with RIPA and this Policy. However, where CCTV is used in the monitoring of public areas in an overt way and just happens to catch a criminal act, then this would not be classified as Covert Surveillance. However, there may be occasions where a covert CCTV System is used for the purposes of a specific investigation or operation, in which case, an application for Directed Surveillance may be required. The advice of the RIPA Monitoring Officer must be sought in such circumstances.
- 9.3 Where use of CCTV is requested by the Police, they will be required to follow Police procedure for obtaining appropriate authorisation. A copy of the Police RIPA authorisation must be provided by the officer requesting such use, and retained on file by the CCTV manager. In the event that the Police state that the authorisation contains confidential material, and may not be disclosed, the Police must provide a letter from the Authorised Officer, confirming the scope and duration of the authority. This **MUST** be provided, prior to the installation of new cameras or the use of existing Council cameras.
- 9.4 The latter systems, if overt, generally fall outside RIPA unless used for a specific investigation where the other criteria for Directed Surveillance are established (see later). It should be noted that to comply with fair processing aspects of the Data Protection Act 1998 there must be proper signage to indicate the use of CCTV surveillance, what the purpose is and who controls it in the vicinity of CCTV cameras.

10 Guidance on Completing the RIPA Forms

- 10.1 The RIPA Forms for requesting, reviewing, renewing or discontinuing Directed Surveillance or a CHIS and Guidance Notes on completing the main RIPA application form for directed surveillance are shown at Annex 8.
- 10.2 Officers should always use the latest version of the RIPA forms and these will be regularly downloaded from the Office of the Surveillance Commissioner or the Home Office website.
- 10.3 Annex 4 summarises the points and tests to be considered by Authorising Officers prior to authorising Directed Surveillance and a brief set of guidelines in the form of a flow chart to be applied in any situation to determine whether authorisation for the proposed activity must be sought are shown at Annex 5 (Directed Surveillance) and 6 (Use of a CHIS).

11 Reporting the Results of a Covert Operation

- 11.1 As surveillance evidence, by its nature, is gained in the course of a criminal investigation, it is not disclosable under a subject access request (s.7 DPA).
- 11.2 In the event that a person is prosecuted, and the surveillance evidence remains unused (e.g. because it was not successful) it must be disclosed to the prosecutor, in accordance with the Criminal Procedure and Investigations Act.
- 11.3 Officers must pay particular attention to 'unused' surveillance product and should consider whether it needs to be marked as *sensitive unused material*, particularly if it might place any third party at risk. **In particular, any material that discloses the use of a CHIS or assistance from a member of the public, should be marked as sensitive and be verbally disclosed to the Prosecutor. The identity of a CHIS must never be noted in disclosure records.**

12 Interception of Communications

[Note: the Human Rights Act 1998 and particularly Article 6 (Right to a Fair Trial) and Article 8 (Right to respect for private and family life) must always be taken into account]

12.1 All interception of communications must be carried out in accordance with the provisions of the Regulation of Investigatory Powers Act 2000 and the Codes of Practice pertaining to that Act. The Authority is allowed to intercept communications if it is done as part of normal business practice, for example:

- 12.1.1 The opening of post for distribution throughout the Authority.
- 12.1.2 The logging of telephone calls, for the purpose of cost allocation, identification of private calls for reimbursement, comparative benchmarking, identification of efficiency savings and identification of misuse of the system.
- 12.1.3 The logging of E Mails sent / Internet access for the purpose of private reimbursement.
- 12.1.4 Logging of calls etc. may also fall outside RIPA if it only records traffic data, as this is not classified as interception of communications.
- 12.1.5 Interception of communication can be made as part of a directed surveillance operation or conduct of CHIS, if one or more of the parties to the communication agrees to the interception.

12.2 Interception of Telephone Calls

- 12.2.1 All Heads of Service receive monthly reports of telephone usage from the Call Management System, including call costs. More in depth information can be provided on request. It is the responsibility of each Head of Service to satisfy themselves that there has been no mis-use.
- 12.2.2 Any employee who uses work telephones for private calls must be made aware that this must only be undertaken with the prior approval of their Head of Service.
- 12.2.3 All premium rate numbers, which include competition numbers, directory enquiries, operator calls and international calls, are barred from the System. There is a global restriction on officers being able to dial premium line numbers. Access to dial mobile numbers requires Head of Service consent and staff must be made aware of this.

12.3 Monitoring of the Internet and Electronic Mail

- 12.3.1 The Council has an "Internet Policy and Code of Conduct" for use by its employees. This is the Policy that sets out employees' responsibilities and liabilities. A copy of the Policy is made available to all employees on the Council's Intranet. With the increasing availability of the Intranet and internal e-mailing facilities, it is important that all employees are made aware of the Policy and that failure to comply with the rules could lead to disciplinary action and may be regarded as gross misconduct.
- 12.3.2 The policy of the Council is to restrict access to certain undesirable Internet sites. Officers are made aware in the document that the Information Technology Unit is able to identify every site visited by an individual and to record details of the visit such as the date, time, nature of site, duration of visit etc. If a complaint of abuse is received,

an individual's use of the Internet may be investigated and appropriate action may be taken within the Council's policies and procedures.

12.3.3 During work times, the content of employees' Emails must be restricted to matters relating to their work and job accountabilities save for personal use permitted under the Council's Policy on private use of electronic communications at work, which is contained within the "Internet Policy and Code of Conduct".

12.3.4 The Council has an "Email Policy and Code of Conduct", which set out how such communication must be used. The document stipulates that misuse of Email may be regarded as a breach of the rules contained within the "Email Policy and Code of Conduct" and that deliberate failure to comply with the rules may result in disciplinary action and dismissal. Officers are also made aware in the Policy that Email usage may be monitored.

12.4 Monitoring on Flexi-time Recording

12.4.1 The Council's system of flexible working hours is set out in the Flexible Working Hours Scheme Guidelines, which are readily available to all officers via the Intranet or from the Human Resources Unit. The Staff identification Card System monitors and records the times when a card is used and consequently may provide a method to check flexi-time recording. All employees who record their flexi-time will do so in the knowledge that such recording can be verified and consequently implicitly consent to the removal of any expectation of privacy.

12.4.2 It is emphasised that use of RIPA for monitoring staff, use of internal Email and the internet and other such monitoring can only be authorised when properly judged to be necessary for the prevention or detection of crime. All other monitoring falls under 'In House Interception' (see below).

12.5 In House Interception, as part of Normal Business Practice

12.5.1 The controller of a telecommunications system must make all reasonable efforts to inform all potential users that interceptions may be made. This will be done by means of: -

- Notification on the Email / Intranet System.
- Inclusion in Council Policies and Procedures, issued to staff.

12.5.2 This will include informing potential users that certain interceptions will be carried out as part of the normal operation of the Council.

- Monitoring internet access
- Monitoring Email usage
- Telephone call logging
- Opening post for distribution

12.5.3 The Council will maintain a register of all interception of communications that will have the following information: -

- Date commenced
- In house / providing assistance to an outside agency
- Level of consent

- File Reference
- Date Authorised – if applicable
- Date ceased

12.6 Maintaining a Record of Interceptions

12.6.1 The Interception Commissioner may wish to scrutinise any interceptions made. To enable this, all pertinent records must be kept securely for a period not less than five years. These are:

- Register of interceptions
- Authorisations

12.7 Intercepted Material

12.7.1 All intercepted material and all copies, extracts and summaries of it must be destroyed as soon as it is no longer needed for any of the authorised purposes.

12.7.2 Such material will be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

13 Examples of Actions that Local Authority Officers Cannot Undertake

- 13.1 If any officer is unclear about whether any activity is categorised as being surveillance and thereby covered by RIPA, they must immediately contact the Council's Head of Legal Services or Head of Audit and Review prior to any action being taken. Failure to do so may render the officer(s) involved subject to disciplinary action.
- 13.2 It is not possible to detail all situations where surveillance activity might be undertaken and what is / is not appropriate. However, the blue guidance boxes throughout this document give some examples of such instances. It is essential when planning and undertaking surveillance activities that legislation and people's human rights are not contravened. Examples of actions that the Authority's officers are **NOT** permitted to undertake in any circumstances are detailed below.

RBWM Officers are not permitted to:

Insist on access: Local authority officers do not have a right of access onto or right to remain on any property or in any premises, without lawful authority. Lawful authority would be the granting of permission by the owner or any person who, at that time, had control of the property concerned. Permission to remain on the land or property must be in the form of a written agreement as per *R v Johnson* because, should there be a disclosure to any party that surveillance has or is being undertaken from the property, there may be violent retribution directed against either the property or the owner of the property. Written permission must include the owner's awareness of the risks involved. The individual who is the owner or occupier of the private or residential premises must give 'informed consent' to the surveillance. Any concerns that they have may allow information about their premises being used being prevented from disclosure during prosecution. The rules of *R v Johnson* must be followed and informed consent should be gained to disclaim their rights for compensation from the Council.

'Bug' phones: Telephones cannot be 'bugged' and telephone conversations cannot be listened into except where one or more parties to the communication consents to the action. Interception of communications without consent cannot be authorised by a local authority in accordance with RIPA.

Intercept private post: Local authority officers do not have the right to intercept post that is clearly identified as being private and personal and not expected to be opened in an employee's absence. For other internal post, there would be implied consent for such interception of communication to deal with matters in an employee's absence for holiday, illness or other reason.

Break the law: Road Traffic Act and Regulations appertaining thereto - RIPA does not authorise officers to breach these sets of legislation. Whilst undertaking surveillance, any failure to comply with a road or traffic sign such as a speed limit, or driving recklessly, carelessly or without consideration to other road users, or failure to maintain their motor vehicle under the Construction and Use Regulations is the responsibility of the officer concerned. There is no statutory defence as for other emergency vehicles e.g. the police, fire services and medical teams, whose compliance with road management legislation or direction would defeat the purpose of the use of the vehicle which they were driving. If proceedings are taken against the officer for such offences, the fact that they were undertaking lawful surveillance is only mitigation.

This list is not exhaustive.

14 Codes of Practice

- 14.1 The Home Office has issued Codes of Practice, which give further guidance on Directed Surveillance, CHIS and the interception of communications. Although they do not have the same force as RIPA, they augment and expand on its implementation.
- 14.2 The Codes of Practice are also considered by any Court or Tribunal interpreting RIPA. They must be readily available to officers working with RIPA, or any member of the public. They are regularly updated and are available on the following website: <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/>

15 The "Policing" of RIPA

- 15.1 RIPA is overseen by Surveillance Commissioners. They are tasked to ensure that RIPA is being applied properly. Inspections are carried out at regular intervals. Information about inspection or the Office of the Surveillance Commissioner can be found at www.surveillancecommissioners.gov.uk
- 15.2 Any person who, being an employee of the local authority or person contracted to carry out duties by the local authority, knowingly or recklessly acts, or fails to act, in a way that tends to, or is likely to, obstruct or mislead any person carrying out the duties of an inspector during an inspection by the Office of the Surveillance Commissioner, may be considered to have committed 'gross misconduct' and be liable to disciplinary proceedings.
- 15.3 In addition, any person aggrieved by the way a local authority carries out covert surveillance as defined by RIPA can apply to a Tribunal under the Act for redress within a year of the Act complained of or any longer period that the Tribunal thinks it just and equitable to allow.
- 15.4 The Tribunal can quash any authorisation and can order the destruction of information held or obtained in pursuit of it.
- 15.5 It cannot, as yet, award compensation, but its findings may be of use in a Human Rights case challenge or as a defence to a case brought by the Council, or in a referral to the local government Ombudsman, or a complaint to the Information Commissioner, from where compensation awards can flow.

16 Consequences of Non Compliance

16.1 Where covert surveillance work is being proposed, this Policy and Guidance must be strictly adhered to in order to protect both the Authority and individual officers from the following:

- 16.1.1 **Inadmissible Evidence and Loss of a Court Case / Employment Tribunal / Internal Disciplinary Hearing** - there is a risk that, if Covert Surveillance and Covert Human Intelligence Sources (both defined at Section 4) are not handled properly, the evidence obtained may be held to be inadmissible. Section 78 of the Police and Criminal Evidence Act 1984 allows for evidence that was gathered in a way that affects the fairness of the criminal proceedings to be excluded. The Common Law Rule of Admissibility means that the court may exclude evidence because its prejudicial effect on the person facing the evidence outweighs any probative value the evidence has (probative v prejudicial).
- 16.1.2 **Legal Challenge** - as a potential breach of Article 8 of the European Convention on Human Rights, which establishes a “right to respect for private and family life, home and correspondence”, incorporated into English Law by the Human Rights Act (HRA) 1998. This could not only cause embarrassment to the Council but any person aggrieved by the way a local authority carries out Covert Surveillance, as defined by RIPA, can apply to a Tribunal – see section 15.
- 16.1.3 **Offence of unlawful disclosure** – disclosing personal data as defined by the DPA that has been gathered as part of a surveillance operation is an offence under Section 55 of the Act. Disclosure can be made but only where the officer disclosing is satisfied that it is necessary for the prevention and detection of crime, or apprehension or prosecution of offenders. Disclosure of personal data must be made where any statutory power or court order requires disclosure.
- 16.1.4 **Fine or Imprisonment** - Interception of communications without consent is a criminal offence punishable by fine or up to two years in prison.
- 16.1.5 **Censure** - the Office of Surveillance Commissioners conduct regular audits on how local authorities implement RIPA. If it is found that a local authority is not implementing RIPA properly, then this could result in censure.
- 16.1.6 **Disciplinary Action** - Failure of officers to comply with this Policy and Guidance is a disciplinary offence under the Council’s Human Resources Policies and Procedures.

17 Complaints Procedures

- 17.1 If any person complains, they should be directed to the Council's Complaints Procedure, and invited to use it if they wish to make a complaint regarding breach of this Policy and Guidance. ANY complaint received will be treated as serious and investigated in line with this authority's policy on complaints. **Regardless of this, the detail of an operation, or indeed its existence, must never be admitted to as part of a complaint. (See paras 10.1 to 10.3) This does not mean it will not be investigated, just that the result of any investigation would be entirely confidential and not disclosed to the complainant.**
- 17.2 Unlawful access or disclosure of information may be a contravention of the Data Protection Act 1998, and may be reported to the Data Protection Commissioner.
- 17.3 The Surveillance Tribunal is available to anyone who believes that their Article 8 rights have been unlawfully breached by an authority using the RIPA authorisation process.
- 17.4 Judicial Review is available to any person who believes their rights have been unlawfully breached outside the scope of RIPA authorisation.

18 Further Information

- 18.1 A list of the Council's Authorising Officers for Covert Surveillance activity is set out in Annex 1 and the special arrangements authorising surveillance where confidential material may be involved is detailed at Annex 3.
- 18.2 The forms for completion for applications, renewals, cancellations and reviews of Directed Surveillance and use of Covert Human Intelligence Sources are on the Council's Intranet.
- 18.3 Annex 4 summarises the points and tests to be considered by Authorising Officers prior to authorising Directed Surveillance and a brief set of guidelines in the form of a flow chart to be applied in any situation to determine whether authorisation for the proposed activity must be sought are shown at Annex 5 (Directed Surveillance) and 6 (Use of a CHIS).
- 18.4 The Home Office Codes of Practice, which give further guidance on Directed Surveillance, CHIS and the interception of communications and which contain a wealth of information can be found at - <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/>. Although they do not have the same force as RIPA, they augment and expand on its implementation.
- 18.5 Annex 7 provides notes of guidance on the role of the RIPA coordinator and Storage of Authorisation Forms.
- 18.6 Guidance notes for the completion of a RIPA form are provided at Annex 8.
- 18.7 Any enquiries about the Policy and Guidance must be referred to the Head of Audit and Review.

ANNEXES

Covert Surveillance

Council's Authorising Officers

The Regulation of Investigatory Powers (Prescription of Officer, Ranks and Positions) Order 2000, which came into force on 25 September 2000, prescribes that in a local authority, authorisations for Directed Surveillance and the use of a CHIS may only be granted to Assistant Chief Officers and the officer responsible for the management of an investigation. These will be designated as "Authorising Officers".

At its meeting of 28 May 2009, Cabinet gave approval for a number of officers to be designated as the Authority's Authorising Officers for covert surveillance activity. These officers must not act as the "Authorising Officers" for Covert Surveillance if:

- The case and surveillance is to be carried out within their own unit;
- For any reason they have a vested interest in the case.

Following a reorganisation, the currently approved officers are listed below.

The RIPA Monitoring Officer will be responsible for maintaining this list. Annex 3 details the special arrangements for authorising surveillance where confidential material may be involved.

Training of Authorising Officers and those Undertaking Surveillance

Authorising Officers **must** receive full training in the use of their powers. They must be assessed at the end of the training, to ensure competence, and must undertake refresher training at least every two years. Training will be arranged by the Head of Audit and Review. Designated Authorising Officers who do not meet the required standard, or who exceed the training intervals, are prohibited from authorising applications until they have met the requirements of this paragraph. Authorising Officers must have an awareness of appropriate investigative techniques, Data Protection and Human Rights Legislation. Those officers who actually carry out surveillance work must be adequately trained prior to any surveillance being undertaken. A Corporate training programme will be developed to ensure that Authorising Officers and staff undertaking relevant investigations are fully aware of the legislative framework. Authorising Officers will **not** be able to authorise surveillance activities until they have received appropriate training.

Approved Authorising Officers

- Chief Executive, Ian Trenholm (including Confidential Information)
- Strategic Director of Environment, David Oram
- Interim Strategic Director of Resources, David Scott
- Head of Finance – Andrew Brooker
- Head of Public Protection – Terry Gould
- Head of Planning and Development, Tim Slaney
- Head of Children's Commissioning, Angela Wellings

Authorisation involving either *Confidential Information* or a juvenile or vulnerable CHIS may only be given by the Chief Executive ('Head of Paid Services') or, in his absence, a Chief Officer who meets the other criteria in this appendix.

R v Johnson Guidance

Private Places (R v. Johnson)

In addition to the RIPA requirements, where officers are using private property as a static observation point, the case of *R v Johnson* introduced the guidelines to say that a senior investigator/ fraud manager must: -

- Ensure that the owner/occupier is visited before the observation takes place;
- Make sure that the owner/ occupier is fully aware of the purpose of the observations;
- Explain that the location of the observation point might need to be disclosed to a court; and
- Gain their informed consent to continue.

Officers must make a record of the interview and their consent in writing. If the case comes to court, a fraud manager or more senior officer must visit the property to: -

- Find out whether the owner/occupier is the same as when the observations took place;
- Tell them what is happening; and
- Record their comments

If they are fearful of the consequences of disclosure of their address, this may give grounds for that information being withheld under Public Interest and Immunity rules.

Covert Surveillance

Special Arrangements for Authorising Surveillance Where Confidential Material may be Involved

Confidential material is particularly sensitive and is subject to additional safeguards. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source is subject to special authorisation. In these cases, the Authorised Officer will be the Head of Paid Services.

An assessment must be made of how likely it is that the confidential material will be acquired.

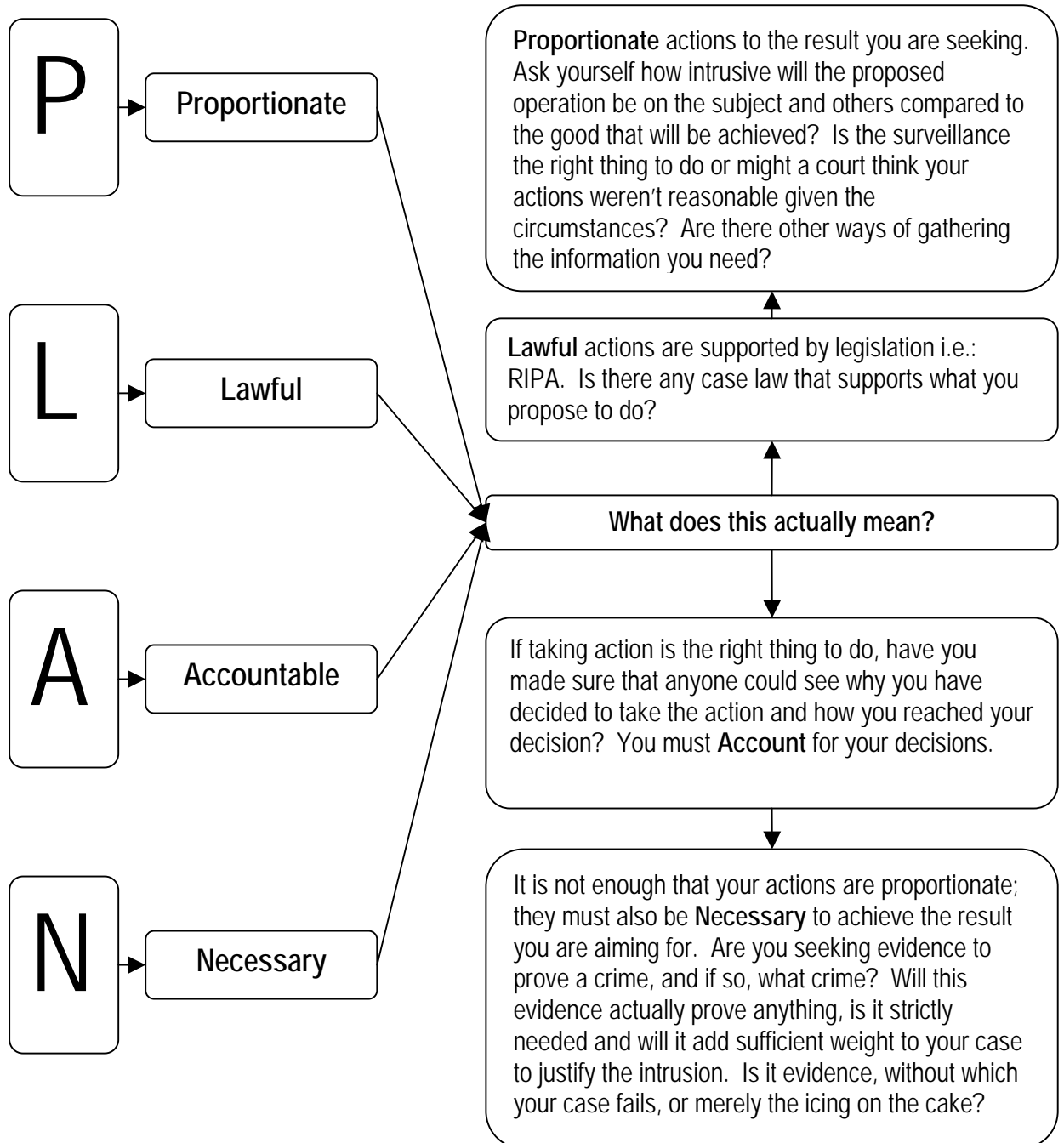
Special care must be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications must only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

The following general principles must be applied:

- Those handling material from such operations must be alert to anything that may fall within the definition of confidential material. Where there is doubt, advice must be sought from the RIPA Monitoring Officer before further dissemination takes place.
- Confidential material must be retained as per CPIA.
- It must be disseminated only where an appropriate officer (having sought advice from the Head of Audit and Review) is satisfied that it is necessary for a specific purpose. Dissemination should be done in accordance with the National Intelligence Model and with the receiving party meeting the specified conditions in the handling code.
- The retention or dissemination of such information must be accompanied by a clear warning of its confidential nature. It must 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 where possession of it might prejudice any criminal or civil proceedings related to the information.
- Confidential information must be destroyed as soon as it is no longer necessary to retain it for a specific purpose. Refer to the DPA, LGFA and CPIA guidelines for retention and destruction of material.

Annex 4

Notes for Guidance for Authorisation Tests – Directed Surveillance



Authorised Officer's Statement

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

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

You must start by fully explaining what operation you are authorising. State why the surveillance is necessary to the case, what will be achieved, how it will be carried out, how many people used, what equipment / vehicles / technology you authorise the use of and where the operation will happen.

Make sure it is clear exactly what it is that you are authorising.

13. Explain why you believe the directed surveillance is necessary. [Code paragraph 2.4]

Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]

Now you must explain your decision. Simply stating that you "agree with the officer who applied for the reasons they gave" is not acceptable. You must give, in your own words, a detailed account of how you came to decide that the operation was necessary and proportionate. Make sure that you review the guidance in section seven and show how the evidence is necessary to the offence, and how the offence is one that it is necessary to investigate. Now ensure that you demonstrate how the officer has shown the need to obtain the evidence to be proportionate, when balanced against the person's expectation of privacy, the privacy of innocent third parties and the seriousness of the offence.

If you have completed a surveillance authorisation worksheet, go back over this as you should have already stated your reasons there.

You must explain why you feel it is in the public interest to carry out the action; is it serious, prevalent in the area, an abuse of position, premeditated? Why do you think that the investigation will be prejudiced without surveillance? Are you certain there is no other obvious and less intrusive way of obtaining the information? Does it need to be done? Record everything in this section.

This section must stand on its own, if you are called to court to justify your authorisation.

Authorised Officer's Statement

<p>14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with 3.1 to 3.12</p>		<p>This section is to be completed only by the Senior Authorised Officer if confidential information might be obtained. They should explain why they felt it to be appropriate for the surveillance to be carried out. To comply with the codes, show how further measures, such as more regular reviews and stricter limitations, have been put in place due to the particularly sensitive nature of the operation.</p>
<p>This should be no more than four weeks from the date of authorisation. If you wish to restrict the length of time an officer may carry out surveillance for, you can use this box to set an early review date.</p>	<p>Date of first review</p>	
<p>Use this box to record dates for review. The normal review period is no longer than every four weeks. It doesn't have to be completed but is useful to do so, especially when a shorter review period is appropriate.</p>	<p>Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete dates after first review are known. If not or inappropriate to set additional review dates then leave</p>	
<p>Name (Print)</p>	<p>Grade / Rank</p>	
<p>Signature</p>	<p>Date and time</p>	
<p>Expiry date and time [e.g.: authorised on 30 June 2005, 23.59]</p>	<p>Authorised on 1 April 2005 - expires</p>	
<p>+++++</p> <p>+++++</p>		
<p>Finally, write your name, sign the form giving the date and time. You must also record the expiry date. This is always three months, to the minute, from the date that the authorisation was given, no longer, or shorter. The operation can be cancelled before this date if appropriate. (See 7.14 (above) for guidance.)</p>		

Sections 15 and 16:

These sections relate to oral authorisations that may be granted or renewed only in urgent cases. In the case that an oral authorisation is granted, the AO should record the reasons why they considered the case urgent and why they believed it was not practicable to delay in order for the investigator to complete an application. Urgent oral authorisations last for seventy-two hours from the time of the authorisation. The officer carrying out the surveillance must complete a written application at the earliest opportunity, not necessarily at the end of the seventy-two hours.

Authorisation will be required for a proposed activity if the answer is **'Yes'** to all of the following questions.

If the answer is **'No'** to any of the following questions, the proposed activity falls outside the scope of RIPA.

1. Is the proposed activity 'surveillance'?

The Officer must decide whether the proposed activity will comprise monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications, recording anything monitored, observed or listened to in the course of the proposed activity and whether a surveillance device will be used.

2. Is it 'covert'?

The Officer must decide whether the proposed activity will be carried out in a manner calculated to ensure that the target(s) will be unaware that it is or may be taking place.

3. Is it 'directed'?

The Officer must decide whether the proposed activity is for the purposes of a specific investigation / operation.

4. Is it likely to result in obtaining private information about this person?

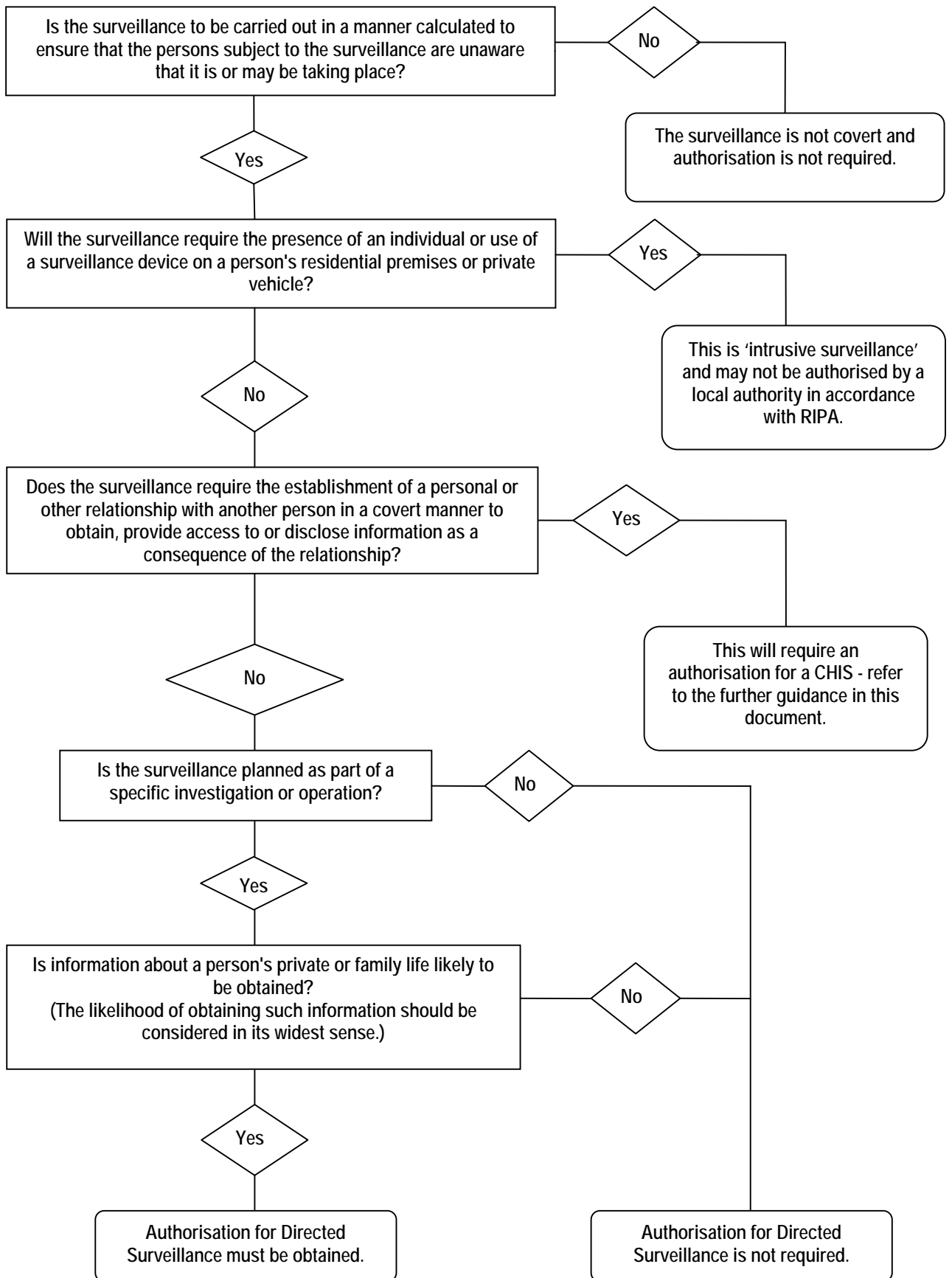
The Officer must decide whether any information about the target's / targets' private or family life is *likely* to be obtained. This test is different from: "Is there the faintest chance that I will obtain private information"?!

5. Is it a 'foreseen / planned response'?

The Officer must decide whether the proposed activity is something other than an immediate response in circumstances where it is not reasonably practicable to get authorisation. If the proposed activity has been planned in advance and not just the immediate reaction to events happening in the course of the Officer's work, it is not unforeseen and requires authorisation if all the answers to questions 1 to 4 have also been 'Yes'.

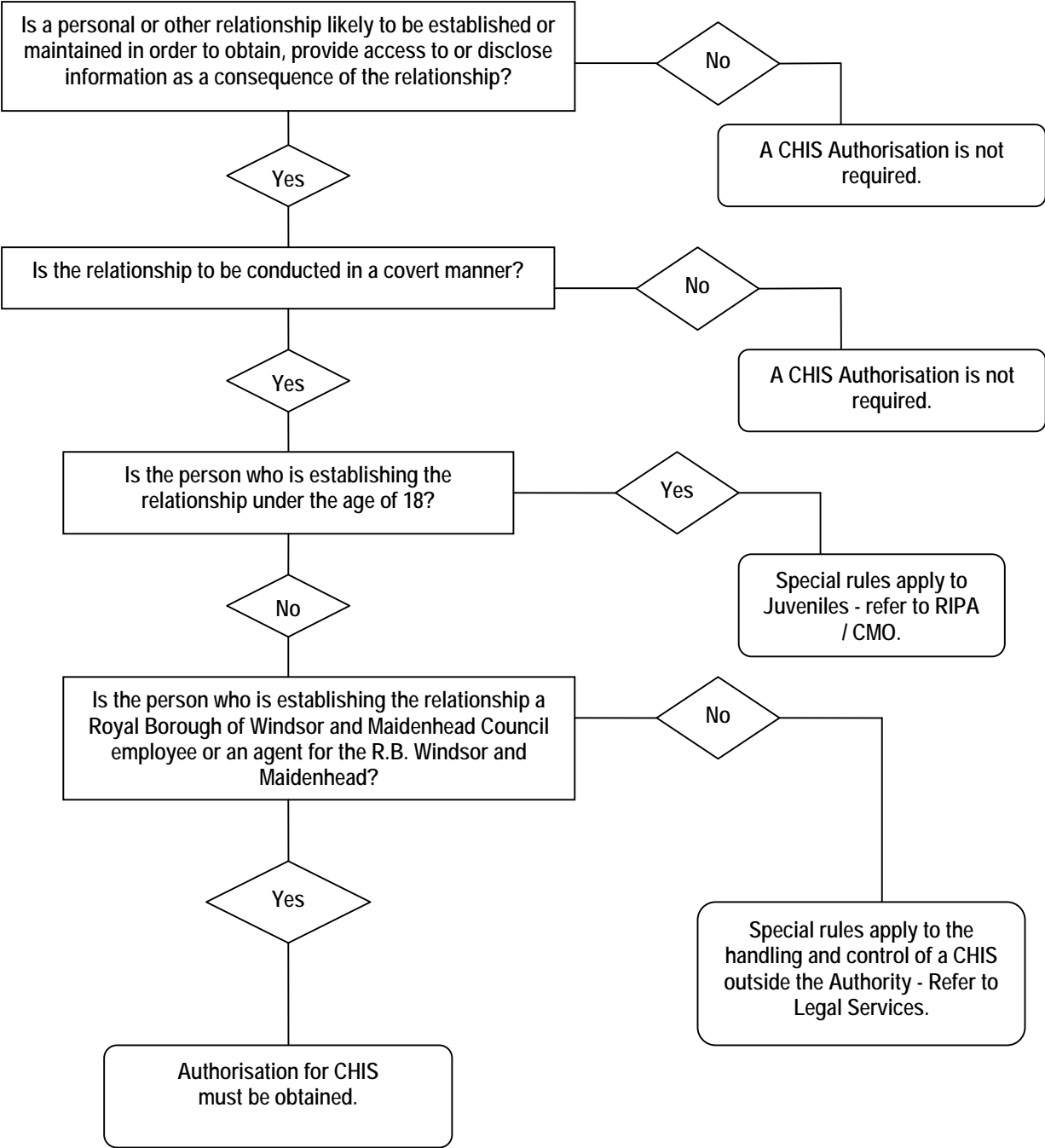
Annex 5

Determination of Whether DS Authorisation is Required



Annex 6

Determination of Whether CHIS Authorisation is Required



Notes for Guidance on the Role of the RIPA Monitoring Officer and Storage of Authorisation Forms

The RIPA Coordinator for the Royal Borough of Windsor and Maidenhead is the Head of Audit and Review, Catherine Hickman. Her contact details are:

Phone: **External: 01628-796233** **Internal: 6233**

Email: **catherine.hickman@rbwm.gov.uk**

The RIPA Monitoring Officer will maintain a register centrally of all authorisations, grants, refusals, reviews, renewals and cancellations. The role of the RIPA Monitoring Officer (RIPA CMO) includes: -

- Reviewing decisions and raising concerns with Authorising Officers (AOs).
- Arranging three or four monthly moderation meetings between AOs so that they can ensure consistency of approach.
- Arranging training and refreshers.
- Keeping records of those allowed to authorise.
- Removing people from list if code not followed / training skipped etc.
- Checking for updated advice (OSC website etc.).
- Drawing to Head of Paid Service and Leader's notice of potential problems.

Each individual authorised officer is personally responsible for reporting the following information to the RIPA Monitoring Officer as soon as possible and, in any event, within one working day: -

- Authorisation of DS / CHIS.
- Review of DS / CHIS.
- Renewal of DS / CHIS.
- Cancellation of DS / CHIS.
- Any unexpected deviations from normal practice or procedure.
- Any unauthorised surveillance operations.
- Any surveillance authorised outside of RIPA.
- Any other matter concerning the authorisation of surveillance that may harm the council's interests.

The RIPA Monitoring Officer will keep the records for three years to comply with Home Office Guidance.

The Authorised Officer should also keep the following. There is no requirement for this to form part of the central register maintained by the RIPA CMO:

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

Records must be retained in accordance with Data Protection principles.

Storage of Authorisation Forms

The Policy makes each Director responsible for organising sufficient systems within their service.

The originals must be retained by the Head of Audit and Review with the Central Monitoring Record. A copy will be returned to the requesting officer for retention on the investigation file. The RIPA Monitoring Officer must be sent a notification of all grants, refusals, reviews, cancellations and renewals of authorisations to satisfy Home Office Code of Practice recommendations.

The RIPA Monitoring Officer will retain records for at least three years after the completion of the investigation. All officers are reminded of Data Protection requirements about retention and storage of documents. If in doubt, advice must be sought from the Head of Legal Services.

The RIPA 1 Form – Guidance Notes on Completion

Directed Surveillance Unique Reference Number (URN) (to be supplied by the central monitoring officer).		Unique reference number. This must be provided by the RIPA CMO
PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000		
APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE		
Public Authority <small>(including full address)</small>	What public body do you work for? Record it here	
	Unit/Branch /Division	What dept / unit do you work in? Record it here.
Full address	Full address of your dept / office / building.	
Contact details	Give a phone number, email address and / or fax number to contact you on.	
Investigation/Operation Name (if applicable)	You can give the operation a name if you wish.	
Investigating Officer (if a person other than the applicant)	If the person who is the investigator in the case is someone other than you, record their name here.	
Details of application:		
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171. For local authorities the exact position of the authorising officer should be given. For example, Head of Trading Standards.		
You must give the position of the Authorised Officer who will be reviewing the application. You do not need to give their name. This should be their full job title, rank or position.		

Page Two

2. Describe the purpose of the specific operation or investigation.	Enter a summary of the reason for the operation and what you are planning to do. Be brief: what will you do, why are you doing it and what will you get out of it?
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.	
4. The identities, where known, of those to be subject of the directed surveillance.	Who are you intending to gather evidence on? If you do not know the identity of all parties you must describe them as best as you are able.
Name: • Address: • DOB: • Other information as appropriate:	
5. Explain the information that it is desired to obtain as a result of the directed surveillance.	What evidence do you intend to obtain from the surveillance? Specify exactly what you intend to get, how much and what types. This is so a judgement can be made on the weight of the evidence that you will get. Be careful what you write here: when you have achieved these aims the surveillance must stop immediately.

What methods will you use for the surveillance? What are the technical aspects? Who, what, when, where, how long, how many, equipment etc. Mention everything. You will not be authorised to do things you don't mention here.

What evidence do you intend to obtain from the surveillance? Specify exactly what you intend to get, how much and what types. This is so a judgement can be made on the weight of the evidence that you will get. Be careful what you write here: when you have achieved these aims the surveillance must stop immediately.

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (SI 2003 No.3171)

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

Cross out the conditions that do not apply to you. In the case of a local authority, the only one that *does* is prevention or detecting crime or disorder.

Specify the offences that you are investigating or preventing. State why the information has to be obtained by surveillance, why do you need it for the reason you specified? How is it essential to the case?

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]

Describe precautions you will take to minimise collateral intrusion

Collateral intrusion is where the operation interferes with the private lives of those not intended to be subject to the surveillance. This could be members of the suspect's family, their partners, colleagues or members of the public. You must identify where there is a risk that you will gather this sort of information. You must take steps to minimise this risk and show that the risk left is unavoidable: what times are you conducting surveillance? Can you avoid catching others on camera? Do you have facilities to remove identifying features? The AO must be satisfied that the need to carry out the operation outweighs this risk.

Page Four

This is where you must justify your actions as proportionate. You should have completed a planner and decided that surveillance is necessary and the last resort. Record here what you have done already and what you cannot do as it'll prejudice the investigation. Tell the AO why the need to carry out the action outweighs the suspect's right to privacy. How serious is the matter? How intrusive will the operation be on the suspect and on others? What might happen if you don't carry out surveillance? Why can't you get the information in other ways? What will be achieved by gathering the evidence?

9. Explain why this directed surveillance is proportionate to what it s
be on the subject of surveillance or on others? And why is this
surveillance in operational terms or can the evidence be obtained
2.5]

...asive might it
by the need for
is? [Code paragraph

10. Confidential information [Code paragraphs 3.1 to 3.12]:

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's details

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

Confidential information is *special knowledge* of a person's religious, political or medical life or information of a confidential journalistic nature (journalistic sources). Communications subject to legal privilege are also confidential. If there is a chance that you might gather this sort of information, indicate the risk here. The authorisation can then only be given by the person within your public body designated by the RIPA code of practice for this purpose.

Finish by giving your name, telephone number, job title or rank. Date the form and sign it.