



-

## **POLICY STATEMENT**

# **Regulation of Investigatory Powers Act 2000 (RIPA)**

Adopted by Cabinet 22 April 2010 [Min.No.179]



## INDEX

### PART 1

1. Introduction
2. External oversight of the Council's RIPA processes - Office of Surveillance Commissioners
3. Senior Responsible Officer (SRO)
4. Authorising Officers
5. Cabinet responsibilities
6. Meaning of covert surveillance
7. Meaning of private information
8. Meaning of directed surveillance
9. For what purposes can the Council conduct directed surveillance and CHIS?
10. Activities/operations involving directed surveillance
11. Activities/operations not involving directed surveillance
12. Covert human intelligence source (CHIS)
13. Activities/operations involving CHIS
14. Activities/operations not involving CHIS
15. Proportionality and necessity
16. Collateral intrusion
17. Collaborative working
18. Legally privileged information, personal confidential information or confidential journalistic material
19. Pending or future criminal or civil investigations
20. Records management
21. Using surveillance equipment
22. Training

### PART 2

Authorisation Procedure for Directed Surveillance and CHIS

### PART 3

Test Purchases

### PART 4

Complaints



---

## **PART 1**

---

### **1. Introduction**

The Regulation of Investigatory Powers Act 2000 (RIPA) and the regulations and orders made thereunder provide the legislative framework within which covert surveillance operations must be conducted in order to ensure that investigatory powers are used in accordance with human rights. This Policy Statement is intended as a practical reference guide for Council Officers/investigators who may be involved in covert operations.

Officers involved in covert operations, must familiarise themselves with the Home Office Code of Practice on Covert Surveillance and Property Interference<sup>1</sup> and the Code of Practice on Covert Human Intelligence Sources, in order to ensure that they fully understand their responsibilities. The Home Office Codes are available from [www.homeoffice.gov.uk/](http://www.homeoffice.gov.uk/)

The right to respect for one's private and family life is enshrined in Article 8 of the Human Rights Act 1998 (HRA) which renders it unlawful for a public authority to act in a way which is incompatible with any of the Convention rights. As with many of the rights in the HRA, the right to privacy is not an absolute right and is subject to certain exemptions.

RIPA and regulations provide an exemption from the right to privacy in certain circumstances, and allow public bodies to interfere with the individual's right to privacy in circumstances which amount to covert surveillance.

The Council is committed to implementing the provisions of RIPA to ensure that any covert surveillance carried out during the course of investigations is undertaken properly and that the surveillance is necessary and proportionate to the alleged offence/s. The Council seeks to ensure that this Policy Statement remains consistent with the Council's objectives.

This Policy Statement ensures:

- that proper procedures are in place in order to carry out covert surveillance;
- that an individual's right to privacy is not breached without justification;
- that the potential invasion of privacy caused by using techniques regulated by RIPA, are properly justified in a clear, concise paper/electronic trail;
- that proper authorisation is obtained for covert surveillance;
- that covert surveillance is considered as a last resort, having exhausted all other avenues;
- that the seriousness of the offence is considered, in addition to the requirement to weigh up the benefits to the investigation, when considering whether to authorise covert techniques under RIPA;
- that an officer is designated as the Single Responsible Officer (SRO) for ensuring that all authorising officers meet the standards required by the Office of Surveillance Commissioners (OSC);
- that Cabinet has a strategic oversight role in/of the Council's RIPA process.

---

### **2. External oversight of the Council's RIPA processes - Office of Surveillance Commissioners**

The Office of Surveillance Commissioner (OSC) aims to provide effective and efficient oversight of the conduct of covert surveillance and covert human intelligence sources by public authorities. The Council is inspected by the OSC, every three years – the last inspection took place in May 2008.

---

<sup>1</sup> The Council has no power to undertake intrusive surveillance operations or enter or interfere with property or wireless telegraphy



---

### 3. Senior Responsible Officer (SRO)

(see sections 3.28 – 3.29 of Home Office Covert Surveillance Covert Surveillance and Property Interference Code of Practice and sections 9.1 – 9.2 Covert Human Intelligence Sources Code of Practice)

The Managing Director is designated the Council's SRO with responsibilities for:

- (a) ensuring the integrity of the Council's RIPA processes;
- (b) ensuring compliance with RIPA legislation and the Home Office Codes of Practice;
- (c) engaging with the OSC when its inspector conducts an inspection;
- (d) overseeing the implementation of any post - inspection plans;
- (e) ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations made by the OSC inspection reports;
- (f) ensuring that concerns are addressed, where OSC inspection reports highlight concerns about the standards of Authorising Officers.

---

### 4. Authorising Officers

(see sections 5.4 of the Home Office Covert Surveillance and Property Interference Code of Practice) and Covert Human Intelligence Sources Code of Practice)

'Director, Head of Service, Service Manager or equivalent' are the terms used for the appropriate level of authorisation within local authorities in the statutory instrument that prescribes the offices, ranks and positions for authorisation purposes (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010). The Council interprets the level of authorisation as follows:

- The Managing Director, Executive Director, Strategic Director and the Regeneration Director are Authorised Officers who may also act in urgent cases.
- Where there is a likelihood that legally privileged, personal confidential information, confidential constituent information between the MP and a constituent or confidential journalistic material will be acquired as a result of a directed covert surveillance operation, authorisation will be by the Head of Paid Service or in his absence, the Executive Director.
- Authorised Officers cannot delegate their function to an Officer who is not authorised by the Order, but 'upwards' delegation is possible.

---

### 5. Cabinet responsibilities

(see section 3.30 of Home Office Covert Surveillance Covert Surveillance and Property Interference Code of Practice and section 3.26 Covert Human Intelligence Sources Code of Practice)

RIPA is a Cabinet function within the meaning of the Local Authorities (Functions and Responsibilities) (England) Regulations 2000.

Cabinet reviews this Policy Statement, on an annual basis, to ensure fitness for purpose. This higher level review provides an additional safeguard against inappropriate or disproportionate use of the RIPA powers.

Cabinet receives reports on the use of RIPA on a quarterly basis, to ensure that RIPA is being used consistently and in accordance with this Policy Statement. Reports are presented in such a way, that individuals and/or organisations who have been/are the subject of an authorisation, are not identifiable.

Cabinet is not involved in making decisions on specific authorisations.

---



## 6. Meaning of covert surveillance

(see sections 1.9 - 1.13 of Home Office Covert Surveillance Covert Surveillance and Property Interference Code of Practice)

Covert surveillance is defined in RIPA as any surveillance which is carried out in a manner **calculated** to ensure that the persons the subject of the surveillance are unaware that it is or may be taking place.

Surveillance includes monitoring, observing or listening to persons, their movements, their conversations, or other activities or communication.

RIPA provides for the authorisation of covert surveillance where that surveillance is likely to result in the obtaining of *private information* about a person.

Investigating Officers need to 'freeze frame' their thoughts just before the moment of surveillance and interrogate their intentions:

- are they trying to be hidden? or
- are they not bothered? or
- do they want the person who is the subject of the investigation to be aware of them?

It may mean investigating officers choosing whether to be preventative or enforcement focussed in a particular situation.

**REMEMBER:** if you are trying to be overt, can you prove this if challenged in Court? Analyse your thought processes and intentions to give you the answers. If your activities are not hidden from the subjects you are investigating, RIPA does not apply.

**The Council only has powers to conduct directed surveillance operations – it does not have the power to undertake intrusive surveillance operations or enter or interfere with property or wireless telegraphy.**

---

## 7. Meaning of private information

(see sections 2.4 - 2.7 of Home Office Covert Surveillance Covert Surveillance and Property Interference Code of Practice)

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

**Private information includes any information relating to a person's private or family life and is taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Private information includes personal data such as names, telephone numbers and addresses. 'Family' is treated as extending beyond the formal relationships created by marriage or civil partnership. Private life considerations can include business premises.**

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public, may still result in the obtaining of private information e.g. CCTV footage of a person attempting suicide released to the media showing the person's photo – the Court held that the people viewing the CCTV footage exceeded to a far greater degree any exposure that would have been caused by an ordinary passer-by and as the person's identity had not been adequately masked in the publicised footage, there was



a serious interference with his private life – the insufficiency of safeguards when compared with the interference with the person’s private life was disproportionate.

Obtaining private information is likely to be the case where a person has a reasonable expectation of privacy even though acting in public e.g. during leisure hours or activities.

As a general rule of thumb, there is a great risk of likelihood of obtaining private information if doing observations around a person’s home. The risk is lessened, but still there, if observing people in public, but during leisure hours or activities. The risk may lessen but still be there around solely commercial premises observed during business hours, as the firm’s employees are made up of private individuals and also by the liberal interpretation by the Courts, of Article 8.

**Base your decision on your knowledge of the site on a case by case basis to determine if you need a RIPA authorisation.**

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

---

### **8. Meaning of directed surveillance**

(see sections 2.2 - 2.3 and sections 2.8 – 2.10, 2.20 – 2.29 of Home Office Covert Surveillance and Property Interference Code of Practice)

Directed surveillance is defined in RIPA as surveillance which is covert but not intrusive and is conducted:

- for the purposes of a specific operation or investigation;
- in such a manner that it is likely to result in the obtaining of private information about a person (whether or not they are the individual specifically identified for the purposes of the investigation or operation);
- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for carrying out surveillance.

---

### **9. For what purposes can the Council conduct directed surveillance and CHIS?**

(see section 5.1 of Home Office Covert Surveillance Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice)

The Council can use directed surveillance or a CHIS only for the purpose of preventing and detecting crime or of preventing disorder.

If a directed surveillance operation does not fall within this purpose, the Council may be acting unlawfully under the HRA. Where an Officer is contemplating undertaking surveillance that does not fall within the RIPA purpose as detailed above, it is recommended that they take advice from Legal Services before they proceed.

---

### **10. Activities/operations involving directed surveillance**

(see Chapter 2 of the Home Office Covert Surveillance and Property Interference Code of Practice)

It is safest to assume that any operation that involves planned covert surveillance of a specific person or persons (including Council employees) likely to obtain private information, of however short a duration, falls within the definition of directed surveillance and will, therefore, be subject to authorisation under RIPA.

The consequence of not obtaining an authorisation may render the surveillance action unlawful under the HRA, or any evidence obtained may be inadmissible in Court proceedings.



It is strongly recommended that Council Officers seek an authorisation, where the surveillance is likely to interfere with a person's Article 8 rights to privacy. Obtaining an authorisation will ensure that the surveillance action is carried out in accordance with the law and is subject to stringent safeguards against abuse.

Proper authorisation of directed surveillance should also ensure the admissibility of evidence under the common law, PACE (Section 78) and the HRA. Directed surveillance must at all times be justified and proportionate and necessary (JAPAN).

The Home Office Code of Practice on Covert Surveillance and Property Interference (see section 2.28) refers to the covert use of overt CCTV and ANPR systems, e.g. where a Council Officer with regulatory responsibilities requests Town Centre Management CCTV operators to track a particular individual who has been identified in the Town Centre undertaking illegal trading or licensing activities. The Code clearly indicates that such targeted directed surveillance activity, should be subject to RIPA authorisation.

Directed surveillance might be used, for example:

- (a) in fraud cases where there is a need to observe a person's home in order to find out who the landlord is, or to find out who the resident has associations with;
- (b) by placing a stationary mobile or video camera outside a building to record antisocial behaviour on residential estates.
- (c) CCTV cameras targeting a particular known offender at the request of the Police in tracking the perpetrator's activities, as part of a pre-planned investigation (NB: if an operation has a number of different potential targets and for the purposes of a specific investigation or specific operation, it can fall within RIPA.
- (d) a person being observed by Environmental Health for running a commercial business of cake making from her home – although the investigation relates to the business, any surveillance is likely to result in the obtaining of private information.
- (f) 'drive by' past a café to establish a pattern of occupancy of the premises by any person – as the accumulation of evidence is likely to result in the containing of private information about that person.
- (g) the use of professional witnesses by the Council to obtain information about an individual.

Surveillance devices do not include standard video cameras, still cameras, or binoculars.

---

## **11. Activities/operations not involving directed surveillance**

(see sections 2.21 - 2.29 of the Home Office Covert Surveillance and Property Interference Code of Practice)

Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. Private information includes any information relating to the person's private or family life. However, it does not include general observation which is part of an Enforcement Officer's normal work.

**General observation** duties of the Council's Enforcement Officers whether overt or covert, frequently form part of their day to day activities and the Council's legislative core functions – such activities will not normally require a directed surveillance authorisation.

### **Examples**

- (a) Enforcement Officer attendance at a car boot sale where it is suspected that counterfeit goods are being sold. In such a case, the Officer is not carrying out surveillance of particular individuals - the intention is, through reactive enforcement, to identify and tackle offenders. The obtaining of private information is unlikely.
- (b) Observing a construction site prior to a visit, or videoing scaffold erectors prior to a visit for the purpose of identifying problems, or stopping on a hill and using binoculars to identify where potential unlawful activities are taking place, do not constitute directed



- surveillance. Similarly, watching premises where it is alleged that alcohol is being sold to children, or making a test purchase, do not constitute directed surveillance.
- (c) The covert recording (with a DAT recorder) by Environmental Health Officers of suspected noise nuisance, where the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels, and the offender is warned\* that if the level of noise continues, recording will occur. In such circumstances, the offender will normally be regarded as forfeiting any claim to privacy.
  - (d) The recording, whether covert or overt, by an Enforcement Officer, of an interview with a member of the public, where it is made clear by the Enforcement Officer that he is a Council employee and that the interview is entirely voluntary. In such circumstances, the person being interviewed knows that the interview is being conducted by a Council Officer and that the information will pass into the Council's possession.
  - (e) Anything which constitutes an **immediate response** e.g. a Council Officer with regulatory responsibilities may by chance be present when an individual is potentially infringing the law and it is necessary to observe, follow, or engage in other surveillance tactics as an instant response to the situation to gather further information or evidence. Once this immediacy has passed, however, any further directed surveillance of the individual, must be subject to RIPA authorisation.
  - (f) Warning\* letters issued to householders about spot checks of their bins and openly carrying out the checks.
  - (g) Sufficient detailed warning letters to alleged perpetrators of the types and timescale of surveillance that may be taken by the Council e.g. Environmental Health leaflets describing surveillance over a three month period by officers/and/or the use of DAT recorders or matron boxes.
  - (h) Where the Council relies on statutory powers such as powers of entry – this negates the need for a RIPA even where the investigation may fit the RIPA criteria.
  - (i) Investigating staff for employment matters.
  - (j) Overt CCTV will not normally require a RIPA as members of the public are aware these are in place and because their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008.
  - (k) Automatic Number Plate Recognition (ANPR) cameras used to monitor traffic flow.
  - (l) In anti-social behaviour litigation cases, where Council Officers ask residents to maintain diary notes of anti-social behaviour incidences.
  - (m) 'Keeping a general eye out' - but note if it is more like 'every Thursday between the hours of 2 and 3a.m. for the next 6 weeks, target cameras in xx spot for 2 people in a white car who throw out old fridges and freezers' is more specific and likely to need a RIPA.
  - (n) 'Drive by' past a café for the purpose of obtaining a photograph of the exterior.

\*Warning letters etc are valid only for 3 months.

Please note that if you have time to think about it, plan it and undertake targeted surveillance on a specific person or persons, you also have the time to consider RIPA requirements and use them when appropriate.

Remember, **IF IN DOUBT GET IT AUTHORISED.**

---

## 12. Covert human intelligence source (CHIS)

(see sections 2.1 – 2.3 and 2.10 – 2.11 of the Covert Human Intelligence Sources Code of Practice)

The use of 'undercover officers' or 'informants' in a covert manner, can on occasions, be a valuable resource for the protection of the public and the maintenance of law and order. A person is a CHIS if:



- h/she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the two bullet points below;
- he/she covertly uses such a relationship to obtain information or to provide access to information to another person; or
- he/she covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

The Council can use a CHIS only for the purpose of preventing and detecting crime or of preventing disorder.

Unlike directed surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. By the very nature of the activity/operation, the use of a CHIS may constitute interference with a person's right to privacy under Article 8 of the HRA (the right to respect for private and family life). It is therefore strongly recommended that the Council considers an authorisation for the use or conduct of a CHIS, whether for the purposes of obtaining information, particularly private information, or simply through the covert manipulation of a relationship.

CHIS will be more commonly used by the Police, HM Revenue & Customs, and intelligence/security services where it is normal practice to use agents, informants and officers working undercover.

**It is important to recognise that in some rare situations, directed surveillance and CHIS may both apply. The use of a CHIS by the Council, is however, likely to be relatively infrequent.**

Remember, **IF IN DOUBT GET IT AUTHORISED.**

---

### 13. Activities/operations involving CHIS

There are occasions, however, when the Council may use a CHIS to obtain information e.g.

- a CHIS may be used as a source to obtain information in respect of an investigation into Housing or Council Tax Benefit fraud; this may be a Council Officer acting undercover.
- a CHIS may be used as a source to obtain information in respect of an investigation into the loss of monies at Council premises where there are cashier activities; this may be a Council Officer acting undercover.
- a professional witness CHIS posing as a neighbour to obtain evidence.

This list is clearly not definitive. There is an element of judgement involved in determining when an individual taking some part in an investigation may be acting as a CHIS and the matter is not entirely black and white; if in doubt take advice from Legal Services.

Please refer to Part 3 of this Policy Statement for guidance on 'test purchases'.

---

### 14. Activities/operations not involving CHIS

The following situations will not normally require a relationship to be established for the covert purpose of obtaining information:

- test purchase transactions carried out in the normal course of business, where Officers do not establish a personal or other relationship e.g. the purchase of a music CD for subsequent expert examination would not require authorisation, but where the intention is to ascertain whether a trader is taking delivery of suspected fakes and a relationship is



established between the trader and the Officer, then authorisation should be sought beforehand;  
the task of ascertaining purely factual information e.g. the location of cigarette vending machines in licensed premises;  
where members of the public volunteer information to an Officer as part of their normal duties;  
where the public call telephone numbers set up by the Council to receive information;  
where members of the public are asked to keep diaries of incidents in relation to planning enforcement or anti-social behaviour – however please note that such activity will be regarded as directed surveillance, requiring an authorisation.

### 15. Proportionality and necessity

(see sections 3.3 – 3.6 of Home Office Covert Surveillance Covert Surveillance and Property Interference Code of Practice and 3.2 – 3.4 Covert Human Intelligence Sources Code of Practice)

**Proportionality** - this is a fundamental principle embodied in the HRA. Officers must be able to demonstrate that a directed surveillance operation or use of CHIS justifies the level of intrusion of privacy that may occur with regard to the target or targets of the surveillance or any other persons i.e. that it is proportionate set against the outcome. Authorising Officers must believe that the activities to be authorised, are **necessary** for the purpose of preventing and detecting crime or of preventing disorder and that the activities are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the target or any other person affected by the covert surveillance, against the need for the activity, in investigative and operational terms.

The reasons why the activity is considered proportionate must be adequately recorded in the application form. It is not enough to simply have a standard phrase saying that the surveillance is proportionate. The rationale for proceeding with covert surveillance needs to be written and explicit. Consider the following in framing responses to questions included in the application form:

- What is the nature of the suspected or alleged offence/infringement?
- Can the size and scope of the proposed activity be balanced against the gravity and extent of the perceived crime or offence?
- What, if any, are the alternatives to covert surveillance, i.e. could the information be reasonably obtained by other means?
- If there are other options why have these been rejected in favour of covert surveillance?
- What is the level of intrusion of privacy likely to be? Minimal? Average? Significant? Interference will not be justified if the means used to achieve the aim are excessive in the circumstances of the case. Further, any proposed interference with a person or persons' private, home and family life (HRA Article 8 rights) should be carefully managed and must not be arbitrary or unfair.
- Is legally privileged, personal confidential information or confidential journalistic material likely to be acquired?
- Is the privacy of other persons not connected with the investigation likely to be effected? (collateral intrusion)?
- What is the desired outcome?
- What is the anticipated benefit to the Council?

Proportionality in this context, has nothing whatsoever to do with whether or not the possible benefits of a covert surveillance operation justifies the time and money expended by the Council, although Officers will no doubt wish to take this into account.

The Authorising Officer will only grant an authority if covert surveillance or CHIS is necessary in the circumstances of the particular case and only for the purpose of preventing and detecting crime or of preventing disorder.



The Authorising Officer will give consideration to alternative means of obtaining the information required e.g. by obtaining statements from witnesses (if available) and will evidence as far as is reasonably practicable, what other methods have been considered and why they were not implemented.

The Authorising Officer will explain how and why the methods to be adopted will cause the least possible intrusion on the target and others.

The Authorising Officer will consider whether the activity is an appropriate and reasonable use of the legislation, having considered all reasonable alternatives of obtaining the necessary result.

**The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary.**

---

### **16. Collateral intrusion**

(see sections 3.8 – 3.11 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 3.8 – 3.11 Covert Human Intelligence Sources Code of Practice)

The Authorising Officer will take into account the risk of collateral intrusion into the privacy of persons other than those who are the direct subjects of the operational investigation, such as innocent bystanders. Measures will be taken wherever practical, to avoid unnecessary intrusion into the lives of those not directly involved in the operation. For example, an investigator may seek to conduct directed surveillance of T, because T is suspected of housing benefit fraud. The surveillance may unavoidably result in the obtaining of some information about T's family members who are not the intended subjects of the surveillance. The Authorising Officer must consider the proportionality of this collateral intrusion and whether sufficient measures are to be taken to limit it, when granting the authorisation.

All applications for directed surveillance and CHIS must include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the Authorising Officer fully to consider the proportionality of the proposed actions.

The same proportionality test applies to the likelihood of collateral intrusion, as to intrusion into the privacy of the intended subject of surveillance.

---

### **17. Collaborative working**

(see sections 3.15 – 3.21 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 3.17 – 3.18 and 6.10 – 6.13 Covert Human Intelligence Sources Code of Practice)

Officers need to be aware of particular sensitivities in the local community where the directed surveillance or CHIS is likely to take place and of any other similar activities being undertaken by other law enforcement agencies e.g. the Police, which could impact on the deployment of surveillance or CHIS.

Where conflicts might arise, the Authorising Officer must consult with a senior officer within the Police force area in which the investigation is to take place.

Where the operational support of the Police or other agencies is foreseen, this must be specified in the authorisation. Directed surveillance or CHIS as part of a joint operation, only requires one authorisation.

---



### **18. Legally privileged information, personal confidential information or confidential journalistic material**

(see sections 4.22 – 4.31 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 4.1- 4.16 Covert Human Intelligence Sources Code of Practice)

'Confidential material' is described by RIPA as being:

- (a) matters subject to legal privilege;
- (b) confidential constituent information between the MP and a constituent in respect of constituency matters;
- (c) confidential personal information; or
- (d) confidential journalistic material.

Approval must be granted by the Head of Paid Service and in his absence, by the Executive Director.

A substantial proportion of communications between a lawyer and client may be subject to **legal privilege**. Matters subject to legal privilege must be kept separate from enforcement investigations or criminal prosecutions, as they will not be admissible in court. In the very rare circumstances where legally privileged information may be acquired and retained, the matter must be reported to the Authorising Officer by means of a review. The Authorising Officer will decide whether the authorisation should continue. The attention of the Commissioner should be drawn to legally privileged information, during the OSC inspection and the material made available to the inspector, if requested.

Oral and written communications are held in **confidence** if subject to an express or implied undertaking to hold the communications in confidence or where such communications are subject to a restriction on disclosure or an obligation of confidentiality contained in legislation e.g. consultations between a health professional and a patient, information from a patient's records or information relating to the spiritual counselling of a person.

**Confidential journalistic material** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to an undertaking. The attention of the Commissioner should be drawn to confidential journalistic material during the OSC inspection and the material made available to the inspector, if requested.

Acquiring material in the manner referred to above, is likely to be rare for the Council.

---

### **19. Pending or future criminal or civil investigations**

(see sections 9.1 and 9.5 of the Home Office CHIS Code of Practice and sections 8.3 and 8.7 – 8.9 Covert Human Intelligence Sources Code of Practice)

Material obtained under directed surveillance or CHIS authorisations, may be used as evidence in criminal proceedings and to further other investigations.

---

### **20. Records management**

(see section 9.3 of the Home Office Covert Surveillance and Property Interference Code of Practice and sections 7.1 – 7.6 and 8.1 – 8.2 Covert Human Intelligence Sources Code of Practice)

The Freedom of Information Act 2000 requires public authorities to maintain efficient record management systems in order to comply with requests for information. Retention periods for information held by the Council, are detailed in the Council's Data Retention Schedule which details Retention periods are based on legal, financial and/or administrative requirements.



All material obtained as a result of having undertaken a directed surveillance or CHIS will be recorded and logged in the investigating officer's notebook in accordance with usual procedures for logging of evidence.

Confidential material will only be disseminated outside the Council where this has been expressly authorised by the Authorising Officer, having taken the necessary legal advice.

Reasonable steps will be taken to ensure that confidential information is securely stored and cannot fall into the wrong hands.

All confidential information (as defined in Part 1, section 18 of this Policy Statement) will be destroyed as soon as it is no longer necessary to retain it for the specified purpose. Regular review of material obtained as a result of covert surveillance will ensure that material is destroyed when its retention can no longer be justified.

The records kept by the Council will be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the directed surveillance target or the CHIS, and the information provided by that CHIS.

The Data Protection Officer ensures that through the Data Retention Schedule, arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance or CHIS. The Council's Records Management Policy details the framework for the management of records within the Council. The Executive Director maintains an overview of the Records Management Policy.

Authorising Officers must ensure compliance with the data protection requirements under the Data Protection Act 1998 and the relevant codes of practice produced by the Council, relating to the handling, storage and destruction of directed surveillance and CHIS material.

---

## **21. Using surveillance equipment**

Officers conducting surveillance must endeavour to use any equipment that is necessary in the conduct of such surveillance in a responsible and discrete manner. Officers should be particularly wary that the use of any surveillance equipment is restricted to being used in a manner that constitutes covert surveillance only. In instances where there is a risk that the use of such equipment will transform the operation into an intrusive one, the surveillance should cease.

Upon the cessation of surveillance, Officers should ensure that any equipment is properly checked upon its return to storage, both as to condition and to ensure that it does not contain material that could fall into the possession of unauthorised staff e.g. staff should ensure that any video tapes, discs etc are removed from the equipment prior to storage and possible use by other persons.

If any faults with the equipment are detected, this should be brought to the attention of the Authorising Officer as soon as possible. Under no circumstances should the Authorising Officer seek to rectify any faults, as this could affect admissibility of the evidence.

---

## **22. Training**

The OSC has emphasised the importance of training in RIPA legislation not least because the views on the legislation can be clouded by inexperience and misconceptions. Lack of training may result in Council Officers having difficulty defending their credentials, if challenged.

All investigators and Authorising Officers are trained on the provisions of RIPA to ensure that the requirements of the law are complied with. Regular update training is provided, to ensure that all personnel involved with the operation of RIPA, are aware of its requirements.



## **PART 2 AUTHORISATIONS PROCEDURE FOR DIRECTED SURVEILLANCE AND CHIS**

---

### **1. What is authorisation?**

(see Chapter 3 of the Home Office Covert Surveillance and Property Interference Code of Practice and Chapters 3- 5 Covert Human Intelligence Sources Code of Practice)

Authorisation is the process by which a directed surveillance operation or CHIS is subject to proper consideration, recording and approval by the Officer conducting the investigation and the Director authorised to approve it.

An authorisation ensures that all relevant factors have been thoroughly considered and checked. It is also the means by which, in the event of challenge, Officers can demonstrate that directed surveillance or the use of CHIS was lawfully conducted and that it was a fair and reasonable way to proceed, despite the possible intrusion of a person or persons' privacy.

As soon as a plan of action is decided upon which involves covert surveillance or the use of CHIS, the appropriate authorisations should be sought. This involves an investigating officer completing the relevant authorisation form at Appendix A.

In general, authorisation should be sought prudently and in advance of the activity constituting the directed surveillance or use of CHIS. In exceptional circumstances, this may not be possible. In circumstances where it is not practicable to secure written authorisation prior to undertaking the activity, for example when fairly innocuous overt surveillance reveals something that needs a directed surveillance immediately, then oral authorisation must be given in advance. Once oral authorisation has been given, a note should be made by the Authorising Officer. As soon as practicable, the investigating officer and the Authorising Officer must ensure that the appropriate form is completed and dealt with in the same way as authorisations obtained conventionally. In any event, oral authorisation must be backed up by written authorisation not more than 72 hours after the oral authorisation was given.

The standard authorisation forms issued by the Home Office and adapted for Council use (Appendix A), cover all of the necessary aspects. It is important that these forms are correctly and adequately completed for all directed surveillance and CHIS operations.

Proportionality, necessity and collateral intrusion are elements of the written application that are of particular importance and an integral part of a number of the questions contained in the standard application forms.

---

### **2. Authorisation procedure**

Must be authorised by the relevant Director as 'Authorising Officer' and requires the personal authority of the Authorising Officer.

1. The Authorising Officer should first satisfy themselves that the authorisation is necessary for the purpose of preventing and detecting crime or of preventing disorder. This is the only ground the Council can rely on.
2. The Authorising Officer should satisfy themselves that the surveillance or CHIS is proportionate to what it seeks to achieve. In many instances, evidence may be obtainable by other routes, other than directed surveillance, e.g. witness statements, official records, the DVLA, etc.
3. The Authorising Officer should consider whether there could be any collateral intrusion on, or interference with, the privacy of person(s), other than the subject of the surveillance. This is particularly relevant where the premises being observed is used by other persons. This must be taken into account by the Authorising Officer



- when considering whether the need for the surveillance is proportionate to the problem.
4. As a matter of policy, no directed surveillance should be carried out by Council staff which may intrude upon circumstances covered by the Seal of the Confession, which refers to the spiritual counselling between a Minister and a member of their faith.
  5. Use the relevant form at Appendix A for an authorisation for directed surveillance or use of CHIS. The form should be completed by the Officer wishing to carry out the directed surveillance or CHIS operation and the Authorising Officer, before any directed surveillance or CHIS operation takes place.
  6. In urgent cases only, authorisation may be given orally, but the form at Appendix B must be completed as soon as possible. In such cases, the Authorising Officer will also need to make a statement to show that they have expressly authorised the surveillance and CHIS, and why it was necessary to give oral approval in the first instance.
  7. Directed surveillance and CHIS might be employed by other agencies with which the Council carries out joint investigations, for example the Police or the Environment Agency. In those instances, care should be taken to determine whether there will be directed surveillance, who by, and who will be authorising its use. It is normally for the tasking agency to obtain or provide the authorisation. If the Council decides that directed surveillance or CHIS is necessary, then it should inform those in the other agencies involved in the joint investigation.
  8. The Authorising Officer should not normally be responsible for authorising operations in which they have been directly involved, although this may on occasion, be unavoidable. Where an Authorising Officer authorises such an investigation or operation, the Departmental file and central data base should highlight this and the attention of the inspector should be invited to it during the OSC inspection.
  9. The Authorising Officer must be satisfied that the appropriate arrangements are in place for the management of the CHIS. This should include a risk assessment for health and safety (see section 6.14 Covert Human Intelligence Sources Code of Practice).
  10. The authorisation for directed surveillance and CHIS and any associated papers (other than confidential information as defined in Part 1, section 18 of this Policy Statement), should be retained on the Departmental file and on the central data base for a period of 3 years from the ending of each authorisation, in accordance with the Data Retention Schedule.
  11. Confidential information (as defined in Part 1, section 18 of this Policy Statement) will be destroyed as soon as it is no longer necessary to retain it for the specified purpose.
  12. The SRO will on request, make the authorisations available for inspection, by the OSC and to the Investigatory Powers Tribunal.
  13. Authorising Officers must ensure compliance with the Data Protection Act 1998 principles.

---

### 3. What is the duration of authorisations?

(see section 5.10 – 5.11 of Home Office Covert Surveillance and Property Interference Code of Practice and sections 5.13 – 5.14 Covert Human Intelligence Sources Code of Practice)

Authorisations for a directed surveillance operation will, (unless renewed or cancelled), cease to have effect at the end of a period of three months beginning with the day on which the authorisation took effect e.g. authorised on 20 December 2009: expires 19 March 2010.

Authorisations for CHIS will, (unless renewed or cancelled) cease to have effect at the end of a period of twelve months beginning with the day on which the authorisation took effect e.g. authorised on 20 December 2009: expires 19 December 2010.

**Urgent oral authorisations** or written authorisations for a directed surveillance or CHIS operation granted by a Director (as the person entitled to act in urgent cases), will cease to have effect (unless renewed) after seventy-two hours beginning with the time the authorisation was granted or renewed.



#### 4. How is an operation reviewed, renewed or cancelled?

(see sections 5.12 – 5.18 of Home Office Covert Surveillance Covert Surveillance and Property Interference Code of Practice and sections 5.15 – 5.24 Covert Human Intelligence Sources Code of Practice)

All directed surveillance and CHIS must be effectively assessed and regularly monitored by the Officer conducting the operation and the Authorising Officer. The authorisation process should be viewed as a useful management tool to help Officers to achieve this. Regular reviews of authorisations should be undertaken to assess the need for surveillance to continue. Responsibility for assessing the appropriate review period rests with the Authorising Officer and this should be as frequently as considered necessary and practicable. There is clear guidance on reviews, renewals and cancellations in the Home Office Codes of Practice and Officers should refer to the appropriate sections for further details.

The standard renewal and cancellation forms issued by the Home Office adapted for Council use (Appendix A), cover all the necessary aspects. It is important that these forms are correctly and adequately completed. It is particularly important at the review stage that renewal or cancellation of an operation is considered.

The Authorising Officer who granted or last renewed an authorisation must **cancel** it, if he/she is satisfied that the directed surveillance no longer meets the criteria upon which it was originally authorised (see below for more details on the rules relating to cancellations).

#### Reviews

Regular **reviews** will take place once authorisation has been granted. Except in exceptional circumstances, the review will take place 14 days after a written authorisation has been granted and 24 hours after an urgent authorisation has been granted. Records of reviews will be maintained in the Departmental file and on the central data base. Records will be retained in both locations for a period of 3 years, from the ending of each authorisation.

#### Renewals/Extensions

It will be rare that **renewals/extensions** of authorisations will be required in order to continue surveillance. However, if they are required, applications for renewals of authorisation will be made in writing using a standard renewal proforma (Appendix A).

If the Authorising Officer considers it necessary for the authorisation to continue, then it may be renewed/extended as follows:

- for an ordinary authorisation, renewed for a period of up to three months;
- for an urgent oral authorisation, renewed for a period of up to 72 hours;
- all applications for renewals/extensions will contain the following information:

renewal/extension numbers and dates of any previous renewals;  
 details of any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal/extension;  
 the reasons why it is necessary to continue with the directed surveillance or CHIS operation;  
 the reasons why the directed surveillance or CHIS operation is still necessary and proportionate to what it seeks to achieve;  
 the content and value to the investigation or operation of the information so far obtained by the directed surveillance or CHIS operation;  
 details of the results of the regular reviews of the investigation or operation.

Permission to renew/extend directed surveillance or a CHIS operation, will be granted on an exceptional basis. No proforma is provided for renewing/extending approvals. The circumstances will be so unique, that it must be argued on a case by case basis.



Records of renewals will be maintained in the Departmental file and on the central data base. Records will be retained in both locations for a period of 3 years, from the ending of each authorisation.

### **Cancellations**

Authority to carry out covert surveillance is valid for a period of 3 months, from the date it was granted. However, there is a duty incumbent upon both the Authorising Officer and the Officer carrying out the surveillance, to continually review its necessity and proportionality. The operation must be **cancelled** as soon as it is no longer appropriate, irrespective of the time outstanding. The cancellation must be recorded in writing on the appropriate authorisation form (Appendix A) and retained in the Departmental file and on the central data base for 3 years from the ending of each authorisation.

As soon as the decision is made to cancel the authorisation, the directed surveillance or CHIS operation must immediately cease.

---

## **5. Security and welfare of the CHIS**

(see sections 3.12, 6.7 and 6.14 – 6.16 of the Covert Human Intelligence Sources Code of Practice)

There are rules about the use of vulnerable adults or juveniles as sources and there are also special requirements with regard to the management, security and welfare of sources. Refer to the Covert Human Intelligence Sources Code of Practice for detailed guidance. In summary:

- (a) when deploying a source, the Council should take into account the safety and welfare of that source, when carrying out actions in relation to an authorisation or tasking, including the foreseeable consequences to others, of that tasking.
- (b) before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences, should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.
- (c) the person responsible for the day to day management of the source's welfare and security e.g. departmental manager, will bring to the attention of the Authorising Officer, any concerns about the personal circumstances of the source, insofar as they might affect:
  - the validity of the risk assessment;
  - the conduct of the source, and
  - the safety and welfare of the source.

Where deemed appropriate, the concerns about such matters should be considered by the Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.



## PART 3

### TEST PURCHASES

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose e.g. an Environmental Health Officer may be involved in the test purchase of items which are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

It is the view of the Home Office that, in the majority of instances, alcohol test purchasing by persons under 18 years of age is not conduct to which authorisations need be applied. Any use of persons aged under 18 to make test purchases must nonetheless be subject to a risk assessment and must take account of the safety and welfare of the child.

In each instance of test purchasing, on a one-off basis, in retail premises accessible to the public, it is reasonable to assume that:

- (a) surveillance is not likely to be conducted in such a way as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation); and
- (b) the test purchaser is not a CHIS because he/she does not establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the obtaining of information. The one-time act of making a purchase in a shop open to the public, where there may even be no verbal exchange, cannot reasonably constitute establishing a relationship, personal or otherwise – other than a momentarily fleeting one in which no information is obtained, which could reasonably constitute an interference with the privacy of the retailer.

Those assumptions are equally valid in circumstances where it is appropriate to evidence systematic breach of licensing legislation at any given licensed premises by using a number of different test purchasers, each making a one-off purchase.

The Home Office does not believe that the use of a covert surveillance or evidence gathering device by either the child test purchaser or an observing Officer alters the position stated above. There are, however, some important qualifications to this advice. Firstly, different considerations would apply where the test purchaser had made previous visits to the premises, or is to make repeated visits, and had established or is to establish a relationship with the retailer prior to the attempted test purchase. Secondly, different considerations would apply, if the attempted test purchase is made other than from retail premises open to the public, for example from a person's home including parts of their home adjacent to retail premises.

If the use or conduct of CHIS is applied even if the test purchaser is not deemed to be CHIS, it is considered good practice to follow the RIPA authorisation requirements to ensure that -

- the safety and welfare of the test purchaser has been fully considered;
- any risk has been properly explained to, and understood by the test purchaser; and
- a risk assessment has been undertaken, covering the physical dangers including any moral and psychological aspects of the test purchaser's deployment;
- a record is kept.

In the vast majority of test purchase operations, it is likely that there will be minimal risk to the test purchaser involved.



It is important that those individuals involved in the planning and conduct of test purchasing exercises avoid inciting, instigating, persuading or pressurising a person into committing an offence that, otherwise, would not have been committed.



## PART 4

### COMPLAINTS

If you have any reason to believe that you have been subjected to unauthorised covert directed surveillance by the Council, or you wish to complain about any other aspect of the Council's operation under RIPA, then you may complain to the Council's Corporate Complaints Officer or to the Investigatory Powers Tribunal.

The Council operates an internal complaints procedure - full details are available on the Council's website [www.dartford.gov.uk](http://www.dartford.gov.uk). Complaints can be emailed to the [complaints.officer@dartford.gov.uk](mailto:complaints.officer@dartford.gov.uk) or posted to:

Corporate Complaints Officer  
Dartford Borough Council  
Civic Centre  
Home Gardens  
Dartford  
Kent DA1 1DR

The Investigatory Powers Tribunal can investigate anything you believe has taken place against you, your property or communications, as long as it relates to a power held by the organisation you are complaining about, under RIPA.

Investigatory Powers Tribunal  
PO Box 33220  
London  
SW1H 9ZQ.  
Tel: 0207 035 3711

Website address: [www.ipt-uk.com](http://www.ipt-uk.com)

These procedures are mutually exclusive. However, you should first attempt to exhaust the Council's complaints procedure before complaining to the Investigatory Powers Tribunal.

Dependant upon the nature of the complaint, the Council may refer you to the Local Government Ombudsman.