REGULATION OF INVESTIGATORY POWERS ACT 2000

GUIDANCE AND PROCEDURE NOTES

August 2006

REGULATION OF INVESTIGATORY POWERS ACT 2000

INTRODUCTION

The purpose of this document is to provide guidance on the operation of the Regulation of Investigatory Powers Act 2000 and to set out the procedures to be followed when seeking authorisations for covert surveillance, for the use of covert human intelligence sources (CHIS), or for accessing communications data under this Act. This Guidance contains the following:-

1. Background to the relevant Acts
2. Covert Surveillance - Definitions
3. Covert Human Intelligence Sources – Definitions
4. Authorisations - Criteria
5. Authorisations for Covert Surveillance- Procedures
6. Authorisations for CHIS - Additional Procedures
7. Authorisations for Accessing Communications Data – Additional Procedures

1. BACKGROUND TO THE RELEVANT ACTS

1.1. It is the responsibility of all public bodies to comply fully with the requirements of the Human Rights Act (HRA) 1998 which came into force on the 2nd October, 2000. The HRA makes rights protected by the European Convention on Human Rights (ECHR) part of UK domestic law. The Regulation of Investigatory Powers Act (RIPA) 2000 was enacted in order to give a clear statutory framework for the operation of certain intrusive investigative techniques, to provide for compliance with the HRA. RIPA also provides for the appointment of independent Surveillance Commissioners to oversee the exercise by public authorities of their powers and duties under the act.

1.2. The purpose of RIPA is to regulate the "interception of communications, the, acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed."

1.3. Essentially RIPA requires the following human rights principles to be complied with in investigatory work:-

- is the proposed action lawful
- is the proposed action proportionate
- is the proposed action necessary
- is the proposed action non-discriminatory.

1.4. To coincide with the RIPA coming into force, the Home Office has published four statutory Codes of Practice, which are mandatory under the terms of the Act (Part IV, para 75(1)), covering:-

* Use of covert surveillance
* Use of covert human intelligence sources
* Interception of communications and accessing communications data
* Investigation of electronic data protected by encryption.

All public authorities (including local authorities) are expected to comply with the Codes.

1.5. Under the Codes of Practice, any proposed covert surveillance, use of human intelligence sources or accessing of communications data has to be properly authorised. An authorisation under RIPA will provide that the relevant surveillance activity is lawful. It will also ensure that proper consideration is given to the rights of the community to privacy under the Human Rights Act. It is, therefore, essential that any surveillance carried out by Council Officers is properly authorised and is conducted in accordance with the terms of that authorisation. This will provide protection for the Council from legal action (for example under the Human Rights Act or Data Protection Act). It will also protect the Council in the event of complaints to the Local Government Ombudsman or to the Investigatory Powers Tribunal.

1.6. In all cases involving surveillance and the possible application of the RIPA requirements, officers should seek advice from Legal Services if they are in any doubt as to how they should proceed.

2. COVERT SURVEILLANCE - DEFINITIONS

2.1. The following definitions apply for the purposes of RIPA:-

a) Surveillance is defined as including:-

- monitoring, observing, listening to persons, their movements, their conversations or their other activities or
- recording anything monitored, observed or listened to in the course of surveillance and
- surveillance by or with the assistance of a surveillance device.

There are different types of surveillance, which may be categorised as:-
- general surveillance or observation (not directed at an individual or for a specific purpose);
- overt surveillance;
- covert surveillance, which may be further categorised as either directed or intrusive

RIPA authorisation is not required for all surveillance. It only applies to covert surveillance. General observation which does not involve systematic surveillance of an individual or which is not directed to a specific purpose will not usually be regulated under the provisions of RIPA. Such observation may involve the use equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras.

b) Covert Surveillance

In terms of RIPA an action is defined as covert if, and only if, it is carried out in a manner that is calculated to ensure that the persons who are subject to surveillance are unaware that it is or may be taking place. Such surveillance can be either "directed" or "intrusive".

c) Directed Surveillance

Surveillance is directed if it is covert, but not intrusive and is undertaken:

- for the purpose of a specific investigation or specific operation. It is not a requirement that a particular person should be identified as the target of such surveillance.

- in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purpose 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 practical for an authorisation under this part to be sought for the carrying out of the surveillance.

d) Intrusive Surveillance

Covert surveillance is intrusive if it is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device (i.e. any apparatus designed or adapted for use in surveillance which would include cameras, tape recorders etc.)

However, surveillance carried out in relation to residential premises by use of a device (i.e. a camera) which is not in or on the premises is not intrusive (although it will be directed) unless it is of the same quality of information as would be obtained if the equipment was in the premises.

RIPA does not cater for the use of overt CCTV surveillance systems, as members of the public are aware that such systems exist. General use of CCTV does not require authorisation. However. If CCTV is utilised for a covert pre-planned operation to follow an individual already identified then an authority should be sought for Directed Surveillance

Intrusive surveillance can only be carried out with the approval of the Surveillance Commissioners as it should only relate to an investigation re serious crime and thus being dealt with by the police.

e) Private Information

This includes any information relating to a person's private or family life. This has been held by the European Courts to include details of relationships; details of a person's home, even if open to public view and details of business, professional or work life. Surveillance of business premises may, therefore, fall within the definition of covert surveillance for the purposes of RIPA.

2.2. Examples of Behaviour which is not covert surveillance

* a visit by an authorised member of staff who announces the reason for their visit and requests entry to the premises

* any information obtained as a result of questions to the resident is not covert surveillance

* any information obtained as a result of observation in the part of premises to which the officer is invited is not covert surveillance

* any information obtained as a result of a request to make an inspection would not be covert surveillance

* the recording of a telephone conversation with the agreement of the other party

* going onto residential premises to take action to address an immediate nuisance is not covert surveillance (it might breach Article 8 but would come within the permitted derogations provided the action could be shown to be proportionate to the harm being caused).

2.3. Behaviour which could amount to Covert Surveillance and "Intrusive" Surveillance

* going onto residential property in the absence of the occupier and looking through windows, in the dustbin, at the contents of a shed etc.

2.4. Surveillance which is not Intrusive

* any surveillance on business premises or vehicles for business use.

3. Covert Human Intelligence Source - Definitions

3.1. A person is a covert human intelligence source if he or she establishes or maintains a personal or other relationship with another person for the covert purpose of obtaining information from that other person. The surveillance is covert if and only if it is carried on in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

3.2. A covert human intelligence source is effectively an inside informant or undercover officer i.e. someone who develops or maintains their relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator. A whistle-blower or member of the public voluntarily providing useful information about a potential offence would not be a CHIS, even if that person is asked to pass on further information. The key is whether there is a relationship between the person obtaining the information and the person who is the source of that information.

3.3. The circumstances in which the Council could be considered to be using a covert human intelligence source is where a householder is requested to provide information about a neighbour and that information is obtained not by personal observation, as in the case of neighbour nuisance, but through subsequent conversations with the neighbour under investigation.

3.4. Asking a neighbour to keep records of nuisance suffered by them would not be using them as a covert human intelligence source, because the person concerned would not be relying on a relationship with the person under investigation to obtain information.

4. Authorisations - Criteria

4.1. The use of directed surveillance or covert human intelligence sources or the accessing of communications data for a particular investigation must be subject to prior authorisation by an officer of a rank or position at least as senior as is specified in Regulations made under RIPA. For local authorities this is "Assistant Chief Officer" or "officer responsible for the management of an investigation". North Wiltshire District Council has determined that such authorisations will be made by the appropriate Team Leader, unless the Team Leader is directly involved in the particular investigation, in which case authorisation will be given by a Strategic Manager.

4.2. An authorisation will provide lawful authority for a public authority to carry out covert surveillance. A covert surveillance operation will not always require an authorisation. However, authorisation is required where the purpose of the covert surveillance (wherever it takes place) is to obtain private information about a person, whether or not that person is the target of the investigation or operation.

4.3. The use of directed surveillance or covert human intelligence sources or the accessing of communications data should only be authorised if the authorising officer is satisfied that:-

4.3.1. the action is necessary for the prevention or detection of crime or the prevention of disorder. This means that consideration should be given to whether the information being sought could be obtained using other, overt, means.

4.3.2. the surveillance is proportionate - the HRA defines a measure or action as proportionate if it:

* impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties)
* is carefully designed to meet the objectives in question
* is not arbitrary, unfair or based on irrational considerations.

This means that the chosen method of surveillance should be the one which is the least invasive of the privacy both of the subject of the surveillance and of any other persons who may caught up in the operation by way of 'collateral intrusion'.

.

4.4. The requirements of the RIPA and the HRA impact on all officers of the Council who undertake investigatory or enforcement activities, including Housing Benefits, Environmental Health, Planning and Internal Audit. The following procedures should be adhered to in the conduct of any covert surveillance.

5. AUTHORISATION PROCEDURES FOR CONDUCTING SURVEILLANCE

5.1. As mentioned above, any covert surveillance carried out by Council officers must be proportionate, lawful, authorised and necessary.

5.2. For any covert surveillance to be lawful, records must be sufficient to prove that RIPA has been complied with. All procedures relating to covert surveillance must be documented on standard forms. These are referred to below and are attached.

5.3. Covert surveillance carried out by an officer of the Council should be subject to prior authorisation by an appropriate Team Leader or Strategic Manager. It should not be authorised by an officer directly involved in the surveillance so that there is independent review of whether the surveillance is necessary and proportionate. In addition, applications to access communications data must be made via the designated Single Point of Contact (SPOC), as set out below.

5.4. Application for authorisation should be made in writing on the standard application forms except in urgent cases and these should include full details of the proposed surveillance and the duration. The Monitoring Officer must be notified of such an application and each such application will be allocated a unique reference number. The application must include full details of :

- a detailed description of the grounds on which the surveillance is considered necessary
- why the action is proportionate to what it seeks to achieve (there must be a clear indication of what alternative methods were considered for obtaining the information required and why these were rejected) .
- the person(s) to be subject to the action
- the action to be authorised (i.e. observation / following and reference to any premises / vehicles involved and whether private / public, residential / business)
- an account of the investigation / operation
- the information which is sought from the action
- the potential for collateral intrusion and a plan to minimise this potential (i.e. the potential impact on other people not involved in the action)
- the likelihood of acquiring any confidential / religious material (medical records, financial records, legal documents etc.). A higher level of authorisation is required in respect of confidential / religious material. In all such cases authorisation should be obtained from the Monitoring Officer.

5.5. Where surveillance is reactive (i.e. an immediate response to an immediate situation) this must be documented within reasonable time of the surveillance, usually the following day where possible.

5.6. The authorising officer must consider whether the proposed surveillance is proportionate, lawful, necessary and non discriminatory. In particular, he or she must consider whether there is any other reasonable alternative overt method of obtaining the information sought. The criteria for surveillance is listed on the application forms. If the proposed surveillance cannot be embraced within the criteria it should not be undertaken.

5.7. Surveillance activity must be proportionate to the offence under investigation. For example suspected theft from the workplace may merit surveillance at work but not at the person's home.

5.8. The appropriate course of action must then be decided in terms of the type of surveillance and hence the appropriate form / course of activity:-

- directed surveillance
- intrusive surveillance - not to be undertaken by local authority
- use of a Covert Human Intelligence Source.

5.9. Intrusive surveillance is only allowed for "serious" crimes. The police can only obtain authorisation for intrusive surveillance from the Surveillance Commissioners and it is not likely that such authorisation would extend to investigations conducted by local authorities.

5.10. Records of any surveillance undertaken should be kept. These should be kept in chronological order detailing who is on the surveillance, where it is and what happens. Where notes cannot be written up at the time of surveillance it should be completed as soon as possible afterwards.

5.11. All alterations in the records should be crossed through and initialled and then the corrected material written to the side in the normal manner. Correction fluid should not be used at any time. Completion of the log should ensure that no empty lines are left where additional information could be written in at a later date. These logs could be used in the event of criminal prosecution and should be kept correctly, signed as true statements, and secure at all times.

5.12. In all cases there is a duty of care to those surveyed. All details and approvals must be kept strictly confidential. The privacy of individuals must not be put at risk and unnecessary information should not be documented i.e. if the observed person was incidentally observed in a private context.

5.13. Record sheets should be kept locked with the rest of the supporting documents for a period of 6 years.

5.14. All authorisations should be held at a central point to facilitate independent examination by the Surveillance Commissioners. Copies should therefore be forwarded to the Monitoring Officer.

5.15. All authorisations must be periodically reviewed to ensure that they remain appropriate. The review period will be decided by the authorising officer, which should be appropriate to the circumstances of the particular case, and it should be recorded on the Authorisation Form.

5.16. In all cases Authorisations last for 3 months and then must be renewed before they expire if that is deemed necessary, provided they continue meet the requirement for authorisation. Authorisation should be cancelled as soon as they are considered to be no longer necessary or appropriate. Forms are available for the cancellation and the renewal of surveillance as required . Copies of completed cancellation and renewal forms should be sent to the Monitoring Officer.

6. ADDITIONAL REQUIREMENTS FOR CHIS AUTHORISATIONS

6.1. In addition to the requirements set out above, there are further procedures to be followed in cases when it is proposed to use a Covert Human Intelligence Source (CHIS).

6.2. Special care should be taken if it is proposed to use as a CHIS a person who is under the age of 18 or who is otherwise vulnerable. Vulnerable individuals are persons who are, or may be, in need of community care services by reason of mental or other disability, age or illness or who are, or may be, otherwise unable to take care of themselves, or to protect themselves against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances.

6.3. Under no circumstances should the use or conduct of a source under 16 years old be authorised to give information against the parents or any person who has parental responsibility for him or her. If proposing to make use of a CHIS who is under 16, the authorising officer must ensure that an appropriate adult is present at any meeting (an appropriate adult means a parent or guardian, person who has assumed responsibility for the wellbeing of the CHIS or in their absence a person responsible who is over 18 who is neither a member of, or employed, by the Council). In such situations, the Monitoring Officer must be advised before any action is taken. In addition a risk assessment must be carried out in accordance with the Regulation of Investigating Powers (Juveniles) Order 2000 SI 2793.

6.4. In all cases involving a CHIS, the case officer will be the nominated source handler with day to day responsibility for:-

(i) dealing with the source.

(ii) directing the day to day activities of the source.

(iii) recording the information supplied by the source.

(iv) monitoring the source's security and welfare.

6.5. The case officer's line manager will be responsible for the general oversight of the use of the source.

6.6. The case officer shall carry out a risk assessment of the activity which the CHIS is being asked to undertake and the likely consequences should the role become known.

6.7. The case officer must bring to the attention of the line manager any information of the personal circumstances of the source that may affect the conduct of the source or the personal safety of the source, and the line manager must decide whether or not a review of the Authorisation is necessary..

6.8. Specific records must be kept in relation to a CHIS which are detailed in the Regulation of Investigatory Powers (Source Records) Regulations 2000. The relevant details which must be recorded are:-

a) the identity of the source;
b) the identity, where known, used by the source;
c) any relevant instigating authority other than the Authority maintaining the records;
d) the means by which the source is referred to within each relevant investigatory Authority;
e) any other significant information connected with the security and welfare of the source;
f) any confirmation made by a person granting or renewing an Authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have, where appropriate, been properly explained to and understood by the source;
g) the date when, and the circumstances in which, the source was recruited;

h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in S.29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under S.29(2)(c).

i) the periods during which those persons have discharged those responsibilities;

j) the tasks given to the source and the demands made of him in relation to his activities as a source;

k) all contacts or communications between the source and a person acting on behalf of any relevant investigating Authority;

l) the information obtained by each relevant investigating Authority by the conduct or use of the source;

m) any dissemination by that Authority of information obtained in that way; and

n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by, or on behalf of, any relevant investigating Authority in respect of the source's activities for the benefit of that or any other relevant investigating Authority.

7 ACCESSING COMMUNICATIONS DATA

7.1 In addition to the general authorisation procedures set out above, any requests to access communications data must also comply with the following requirements.

7.2 Access to communications data by local authorities is only permitted where it is necessary for the prevention or detection of crime or the prevention of disorder. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve i.e. it should not be authorised where less intrusive means can be used to further an investigation.

7.3 Local authorities are only entitled to access 'communications data' which falls within the definitions of section 21 (4) (b) and (c) of RIPA. These are:-

(b) any information which includes none of the contents of a communication and is about the use made by any person-
(i) of any postal service or telecommunications service; or
(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

7.4 Local authorities are not entitled to access communications data falling with section 21(4) (a) of RIPA, which covers any traffic data comprised in or attached to a communication. local authorities may only seek to gain access to communications data falling within section 21 (4) (b) and (c) of RIPA.

7.5 All requests to obtain communications data must be made in writing on the appropriate application form and be submitted to the Designated Person (currently the appropriate Team Leader or Strategic Manager if the Team Leader is directly involved in the investigation concerned). Authorisation must only be granted where access to communications data is believed by the Designated Person to be necessary and proportionate.

7.6 If the request is authorised, the Designated Person must then pass the form to the Council's SPOC. On receipt of the Form, the SPOC will allocate to it a unique reference number. Any person acting as a SPOC must have been appropriately trained and accredited by the Home Office.

7.7 The role of the SPOC is to:

- assess whether it is reasonably practicable to obtain the communications data requested,
- to advise applicants/authorising officers on the types of communications data that can be obtained;
- to check that the Form is properly completed and authorised;
- to assess any cost and resource implications to both the Council and the service provider, and
- to liaise with the service providers on obtaining the communications data requested.

7.8 The SPOC may refuse the application if he/she considers that the application has not been properly made or that it is not reasonably practicable or possible to obtain the communications data requested.

7.9 If the SPOC is satisfied that the application has been made properly, and that the required communications data can reasonably be obtained, the SPOC will fill in a Notice in the prescribed form. This Notice must also be signed by the Designated Person before it can be served on the service provider. Once this has been done, the SPOC will serve the Notice on the Service Provider. Any disclosures of communications data will be made by the service provider to the SPOC, who will then refer any relevant information to the applicant.

8.10 A Notice to obtain data from the service provider is valid for a period of one month from the date of the Notice. It can be renewed within that month if a fresh authorisation is made, following the same procedure as that outlined above for the original application.

8.11 The SPOC will record the outcome of the application and will retain as a record, the application form and notice. The SPOC will also record any cancellations of authorisations. Such records must be retained by the SPOC until such time as they have been audited by the Office of Interception Commissioners. A copy will also be passed to the Council's Monitoring Officer to be retained in a central register.

8.12 The Designated Person must cancel authorisations if the obtaining of communications data is no longer necessary or proportionate. He/she must inform the SPOC in writing, who will then cancel the Notice served on the service provider. The cancellation must be recorded on the original application form retained by the SPOC.