

BABERGH DISTRICT COUNCIL

FROM: Acting Head of Legal and
Administrative Services

REPORT NUMBER **E277**

TO: STRATEGY COMMITTEE

DATE OF MEETING 9 February 2006

**CONSIDERATION OF POLICY STATEMENT AND CORPORATE GUIDANCE IN
RELATION TO THE REGULATION OF INVESTIGATORY POWERS ACT 2000**

1. **SUMMARY**

The Committee is asked to consider the adoption of the attached Guidance and Policy Statement (Appendix (A)) in respect of the Regulations of Investigatory Powers Act 2000 (RIPA)

2. **RECOMMENDATIONS TO COUNCIL**

- 2.1 That the Guidance on Authorisation under the Regulation of Investigatory Powers Act 2000 and associated Policy Statement be adopted.
- 2.2 That the RIPA Working Group carry out an annual review of the Guidance and Policy Statement in response to the operational needs of the organisation.

3. **FINANCIAL IMPLICATIONS**

- 3.1 None

4. **KEY INFORMATION**

- 4.1 The purpose of RIPA is to regulate surveillance by public agencies, in order both to protect the public from breaches of the Human Rights Act 1998 and to provide a framework in which those agencies may carry out properly considered and authorised investigation.
- 4.2 The Council carries out only one of the three types of surveillance regulated by the Act, this being known as “Directed Surveillance”. An example of Directed Surveillance would be the covert monitoring of a private residence for noise nuisance or anti-social behaviour (as part of a specific investigation). Surveillance may be carried out in respect of various Council functions, e.g. environmental health, planning enforcement and revenues and benefits.
- 4.3 In the current financial year, Babergh has given 4 authorisations so far. Examples of these are:
- Installation of sound recording equipment in a property to monitor noise nuisance from neighbours. The subject was unaware of the equipment.
 - Installation of video cameras to observe/gather evidence of anti-social behaviour. Again, the subjects were unaware.
- 4.4 The Guidance has been drafted in response to recommendations arising from an inspection by the Office of Surveillance Commissioners in June 2002. A draft document was presented at a follow up inspection in September of this year. The document was approved in principle by the inspectors, with a number of revisions suggested. Those revisions have now been made.

4.5 One of the Inspector's recommendations at the 2005 inspection was that a "forum of operational staff" be established to monitor the Council's performance under RIPA. The group set up to fulfil that role is the RIPA Working Group.

4.6 See also sections 1.1, 1.2 and 1.4 of the Guidance (Appendix (A))

5. **APPENDIX**

(A) Draft Guidance and Policy Statement

6. **BACKGROUND PAPERS REFERRED TO:**

(a) Office of the Surveillance Commissioners' Report 2002

(b) Office of the Surveillance Commissioners' Report 2005

Kathryn Seward
Acting Head of Legal and Administrative Services

CONTACT: Caroline Whatling

DIRECT LINE: (01473) 825717

BABERGH DISTRICT COUNCIL

D R A F T

**GUIDANCE ON AUTHORISATION UNDER
THE REGULATION OF INVESTIGATORY
POWERS ACT 2000 (RIPA)**

BABERGH DISTRICT COUNCIL

POLICY STATEMENT ON SURVEILLANCE

This Council will ensure that all directed surveillance (DS) undertaken by its officers will be conducted in accordance with the statutory guidance issued by the Home Office and practical advice from the Office of the Surveillance Commissioner (OSC). By adopting this approach the Council is endeavouring to ensure that there are no breaches of the Human Rights Act 1998 or of the Regulation of Investigatory Powers Act 2000 (RIPA) itself. The implications of not observing the legislation, or failing to put in place adequate procedural safeguards or to provide clear guidance for officers are:

- damage to the public's perception of the way the Council conducts itself in investigatory activities (i.e. that it abuses its statutory powers) leading to a general loss of confidence
- possibility of increased complaints and compensation claims to the Council
- loss of or challenge to evidence in a prosecution
- penalties imposed by the OSC (including loss of powers)
- possibility of complaints to the Investigatory Powers Tribunal & consequent penalties
- actions against the Council under the Human Rights Act.

This policy statement has been designed to protect both residents of Babergh District and officers that are likely to be involved in statutory duties which involve investigation and/or enforcement.

Steps Taken

The Council has introduced the attached Guidance for Officers. A Central Register of RIPA authorisations is held in Legal Services (together with copies of all authorisations given). The Council has nominated the Head of Legal & Administrative Services as being the responsible officer for ensuring the proper administration and adoption of relevant procedures. The Council has also nominated the Assistant Solicitor as the central monitoring control for the application of the guidance and the completion of the relevant documentation and registers. A forum comprising legal advisers, authorising officers and operational staff will meet regularly to monitor procedure and performance and note any developments in the law.

The Council will ensure that records pertaining to DS are retained, according to its Document Retention Policy, for a minimum of 7 years.

The Council will not use Covert Human Intelligence Sources (CHIS). The Council will only use DS as a last resort. Wherever practicable, the Council will use overt surveillance techniques, thereby keeping the need for authorisation under RIPA to a minimum. Any surveillance is only to be carried out where it is both necessary and proportionate, having properly considered the human rights of the subject.

INDEX

PART 1 – General Framework & Procedure

- 1.1 Introduction
- 1.2 Aim of the Guidance
- 1.3 Surveillance covered by the Act
- 1.4 How does the legislation work?
- 1.5 Safeguards to be used when undertaking surveillance
- 1.6 Use of material in evidence
- 1.7 When do council officers need to get authorisation?
- 1.8 Use of Technical Equipment
- 1.9 Authorising Officers
- 1.10. How is an application for authorisation made?
- 1.11. Duration of Authorisations
- 1.12. Renewal of Authorisation
- 1.13. Reviews and cancellations of authorisations
- 1.14. Forms
- 1.15 The Role of an Authorising Officer
- 1.16 Proportionality
- 1.17 What records must be kept?
- 1.18 Who keeps the records/central register of authorisations?
- 1.19 Breaches of RIPA, its Codes of Practice and the Human Rights Act
- 1.20 Obtaining further guidance

PART 2 – Procedural Flowchart

RIPA Flowchart - Authorisation, Review & Cancellation Procedure

PART 3 – Forms

Forms for Authorisation, Review, Cancellation and Renewal for Directed Surveillance

PART 1

1.1 Introduction

The Regulation of Investigatory Powers Act 2000 (“the Act”) was introduced to regulate surveillance by public agencies so that investigation carried out by those agencies with a view to law enforcement, or in the public interest generally, would not lead to breaches of the Human Rights Act 1998. The legislation protects i) officers carrying out investigatory activity (in the sense that where surveillance is properly authorised and carried out according to the authorisation, the investigator should be protected against claims of unlawful activity); ii) the subjects of surveillance; and iii) the wider public who may be caught up ‘collaterally’ in an investigation.

BDC from time to time carries out monitoring or investigation of personal and commercial activities which may constitute surveillance for the purposes of Part II the Act (the only part to which this Guidance relates). For example:

- Housing Services may wish to monitor a tenant following a complaints of loud music or anti-social behaviour, potentially with a view to court proceedings
- the Council’s internal auditors might undertake observations of staff to see if there is an abuse of their official position
- the Licensing Team may wish to run covert “test bookings” for private hire vehicles
- the Benefit Fraud Team may monitor the personal activities of a suspect
- Environmental Services may wish to investigate food hygiene procedure in a restaurant as part of the Council’s law enforcement function.

This Guidance is issued with a view to implementing a standard council-wide procedure for authorisation of covert surveillance under the Act.

1.2 Aim of the Guidance

This Guidance is intended to:

- a) protect the residents of Babergh by ensuring that all directed surveillance undertaken by BDC will be conducted in accordance with the Act, statutory guidance issued by the Home Office and practical advice from the Office of the Surveillance Commissioner;
- b) remind officers of the key provisions and effects of Part II of the Act; and
- c) set out how and when authorisation should take place at BDC (including provision of relevant documentation and identification of Authorising Officers)
- d) advise on the review and cancellation procedures which follow an authorisation.

This Guidance should be read and used in conjunction with the Act and the Codes of Practice on the Use of Covert Surveillance and Covert Human Intelligence Sources. There is more information on how to access the Act and the Codes in section 1.19 of this Guidance. The Council has decided that as from September 2005, CHIS will no longer be authorised as OSC Inspectors did not recognise a need for CHIS to be a part of the Council's enforcement activities. However, this guidance will cover CHIS to some extent, so that officers can recognise this type of surveillance. If officers determine that there is a need for CHIS, the decision not to authorise will be reviewed.

1.3 Surveillance Covered by the Act

The Act identifies 3 categories of covert activity which may be authorised if the correct procedure is followed:

i) Directed Surveillance (DS)

This is covert but *not intrusive* (see iii below) surveillance, which is undertaken for a specific investigation or operation (rather than as an immediate response to events or as part of a routine patrol) in a way likely to obtain private information about a person.

“**Covert**” surveillance, according to RIPA s.26(9)(a) occurs if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.” If an officer's activities are not hidden from the subjects of their investigation, then those activities are not within the RIPA framework, e.g. spotchecks on dustbins in a recycling scheme. An example of **covert** surveillance would be the monitoring of the movements of a benefit fraud suspect, to determine whether the suspect had undeclared work, or an undeclared person sharing his or her property.

“**Private information**” in relation to a person includes any information relating to his private or family life. According to the results of the 2005 OSC inspection all of the surveillance carried out by BDC is “Directed Surveillance”. The Act says that DS can be authorised by a “designated person”, which in a Local Authority must be an Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent. A list of designated officers at BDC can be found below in the section 1.8 ‘Authorising Officers’.

ii) Covert Human Intelligence Sources (CHIS)

This category covers the use or conduct of someone who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information i.e. any informant, undercover agent or officer. CHIS activity involves covertly using such a relationship to obtain information or provide access to information or covertly disclosing information obtained by the use of such a relationship. A full explanation of what constitutes CHIS is covered by RIPA s26(7)(8) and (9). As indicated above, BDC no longer authorises CHIS. However, in order that Babergh officers do not inadvertently create or use a CHIS, the following guidelines are suggested to enable officers to identify and thereby avoid a CHIS:

- A purpose is covert in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner calculated to ensure that one of the parties to the relationship is unaware of that purpose; and
- A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.
- This clearly covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses retained by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

- Inducing anyone to act in a covert way (see also section 48 RIPA) that is covered by the above definitions would also count as use of a CHIS.
- If in doubt seek advice from Legal Services.

iii) Intrusive Surveillance (IS)

This is covert surveillance carried out on any residential premises or in any private vehicle. It involves a person actually on the premises or in the vehicle or is carried out by a surveillance device on the premises or in the vehicle. It can also include recordings made by a device not actually on the premises or in the vehicle but which give recordings of a quality equal to that which might be obtained from a device on the premises or in the vehicle. A local authority may not authorise Intrusive Surveillance. Authorisation can only be given by a Senior Authorising Officer or by the Secretary of State. Examples of Senior Authorising Officers are: within the police force - certain Chief Constables or Commissioners, within the National Criminal Intelligence Service and National Crime Squad a Director-General and specially designated officers within HM Customs & Excise. In all but the most urgent cases approval from a Commissioner (at the Office of the Surveillance Commissioner – the body which oversees compliance with the Act) is required to be notified to the Senior Authorising Officer before an IS authorisation can take effect. As a local authority may not authorise IS, no further reference will be made to it in this Guidance.

Authorisations for DS do not have to be notified to the Office of the Surveillance Commissioner but must be available for review when Commissioners, Assistant Commissioners and Inspectors visit the authority. This guidance is intended to deal with DS only. It should be noted that there are further regulations for the interception of telephone calls and electronic communications. Again, any officer considering this type of activity should contact Legal Services for specific advice.

1.4 How Does the Legislation Work?

The provisions of the Act, when properly used, effectively counter the provisions of the Human Rights Act 1998, s6 of which makes it unlawful for a public authority to act in a way which is incompatible with the European Convention on Human Rights, in particular Article 8, which stipulates the right to respect for private and family life. The Act allows specific types of surveillance (DS, CHIS & IS) for specific purposes e.g. for preventing or detecting crime or preventing disorder (the only ground now relevant to local authorities), or (by public agencies *other than local authorities*) for the purpose of public safety or for the protection public health PROVIDED THAT the investigations are authorised by a Designated Person or (for a more intrusive level of surveillance) by a Senior Authorising Officer (see explanation of these terms in section 1.3 (iii) above) or the Secretary of State.

Authorisation must be obtained in advance for each investigation.

Broadly, the Act provides that surveillance will be lawful if an authorisation has been properly issued and a person acts in accordance with that authorisation. This is important because:

- a) a person acting in accordance with a duly issued authorisation will be protected from civil liability, and
- b) if the Council is involved in any proceedings before the Court the Council will be able to show that it has acted lawfully and that it has gathered evidence properly.

Compliance with the Act is overseen by the **Office of Surveillance Commissioners** and its inspectors who have been appointed to provide independent monitoring of the use of powers contained in RIPA Part II. They will inspect the Council from time to time to ensure that it is complying with the Act. In addition there is an independent tribunal which has full powers to investigate and decide any case where a person complains about the conduct of the Council in exercising its powers of surveillance.

A lack of authorisation does not *necessarily* make the surveillance unlawful, but the consequences are that:

- evidence gathered may not be admissible in court
- victims of breaches could bring their own proceedings or defeat proceedings brought by the Council on human rights grounds (e.g. as an infringement of Article 8 of the European Convention of Human Rights)

1.5 Safeguards to be used when undertaking surveillance and granting authorisations

Authorisations must be granted on the correct basis or they will not be effective: the Act says that an authorisation should not be granted unless:

- a) it is **NECESSARY** : - to prevent or detect crime or prevent disorder

and the Council is satisfied that the surveillance is undertaken in connection with a statutory function with which the Council is charged; AND

- b) the surveillance is **PROPORTIONATE** to the aim to be achieved. (More guidance on proportionality can be found in section 1.15 below). Broadly, this means that if the surveillance is likely to intrude on someone's human rights, for example the right to respect for private and family life, home and correspondence, that such interference can be justified. It should not be unfair or arbitrary, or have too great an impact on the intended subject. AND
- c) the surveillance is **PROPERLY AUTHORISED AND LAWFUL**. Officers carrying out surveillance shall be properly authorised by the correct person and shall not interfere with any property or harass any person.

More specific guidance to help an Authorising Officer to establish whether a decision is in line with these safeguards is given in sections 1.14 and 1.15 below. Finally – the Authorising Officer should ensure that accurate records of authorisations must be kept. For more information see section 1.16 below.

1.6. Use of material in evidence

Often surveillance will be carried out simply to monitor a situation, but sometime the results of the investigation can provide evidence which may form the basis of court proceedings. This is another reason to ensure that the correct authorisations take place. As indicated above only the product of properly authorised surveillance can be assured of admissibility in court.

1.7 When do council officers need to get authorisation?

In the past, the Suffolk Environmental Protection Group has issued guidance to Environmental Health Officers which suggests that provided subjects are notified in advance that surveillance will be taking place, then the surveillance will not be covert and therefore does not require authorisation under RIPA. This has formed the basic approach made by the Council in the past.

However, it is difficult to gauge how specific this advance warning needs to be in order to satisfy the Office of Surveillance Commissioners; i.e. will the subject need to be notified *on each separate occasion* that surveillance takes place or is a vague written warning that 'surveillance might take place at any time in the next 3 months' sufficient?

Another reason that RIPA authorisations have not so far been requested widely for DS in Council investigations is that it is defined as being 'likely to get private information about a person whether or not they are targeted for the purposes of the investigation or operation'. Because many of the council's investigations are not *seeking* 'private' information as such, but only evidence of e.g. excessive noise, it has not been thought that RIPA authorisation was needed. However, the risk of any investigator picking up incidental or 'collateral' (interference with the privacy of subjects other than the subjects of the surveillance) private information is very high.

In the light of the uncertainty surrounding these issues the corporate position is to take a 'better safe than sorry' approach and consequently all pre-planned surveillance:

- where the subject is not notified in advance on the same day that the surveillance takes place
- whether the *aim* of the investigation is to obtain 'private' information or not

WILL require RIPA authorisation

Specifically, it is suggested that any use of recording equipment (still camera, video, audio) not notified to the subject 'on the day' should be DS authorised. Use of any 'hidden devices' should be considered carefully to ensure this does not constitute 'intrusive' surveillance. In case of doubt, seek specific guidance from Legal Services.

1.8 Use of Technical Equipment

BDC needs to have a policy for the retention and deployment of all covert surveillance equipment. Such equipment should only be used by RIPA trained officers.

Covert surveillance equipment will only be installed with the authorisation of the Council's authorising officers. This will only be used in residential premises if a member of the public has made a complaint or requested help and the matter can only be investigated with the use of covert surveillance techniques. If a resident is requested to keep a video diary as part of an evidence gathering exercise, this will be regarded as directed surveillance on behalf of the Council, and as such will require authorisation.

1.9 Authorising Officers

Authorisation within the Council may only be given for DS. . The following have been nominated as Authorising Officers:

Chief Executive Officer
Mike Hammond, Corporate Director
Head of Revenues Division
Head of Environmental Services Division

An Authorising Officer should not be responsible for authorising their own activities, i.e. those operations or investigations in which they are directly involved or for which they have direct responsibility. It is therefore advised that authorisation be given by a Head of Service other than of the Division where the application originates.

Where "Confidential Information" is to be or may be acquired or a vulnerable individual or a juvenile is proposed to be used as a CHIS (see Home Office Codes of Practice) authorisations may only be given by:

Chief Executive Officer, or in her absence only another Corporate Director

1.10 How is an application for authorisation made?

An application for authorisation for Directed Surveillance must be made in writing. It should specify:

- The action to be authorised
- The identities, where known, of those to be the subject of Directed Surveillance
- An account of the investigation or operation
- The reasons why the authorisation is sought (i.e. the prevention or detection of crime or the prevention of disorder)
- Why the surveillance is considered to be proportionate to what it seeks to achieve
- An explanation of the information which it is desired to obtain as a result of the authorisation
- The potential for collateral intrusion, i.e. interference with the privacy of persons other than the subjects of the surveillance, and an assessment of the risk of such intrusion or interference
- The likelihood of acquiring any confidential material
- Where authorisation is sought urgently, reasons why the case is considered to be urgent

The Authorising Officer must give authorisations in writing, except that in urgent cases, they may be given orally by the authorising officer or officer entitled to act in urgent cases. (In such cases a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant as soon as reasonably practicable).

Additionally, in urgent cases, the authorisation itself must record the reason why the Authorising Officer considered the matter so urgent that oral instead of written authorisation was given.

1.11 Duration of Authorisations

DS a written authorisation will cease to have effect (unless renewed) at the end of a period of 3 months beginning with the date on which it took effect. Exceptionally, an oral authorisation may be given in cases of urgent necessity, in which case the detail referred to above should be recorded in writing as soon as reasonably practicable, and such authorisations will cease to have effect after 72 hours beginning with the time the authorisation was granted.

1.12 Renewal of Authorisation

If at any time before an authorisation ceased to have effect the Authorising Officer considers it necessary for the authorisation to continue for the same purpose for which it was given, then he/she may renew it in writing for a further period beginning with the day when the authorisation would have expired but for the renewal. The renewal will normally be for three months in the case of DS. The request for a renewal of authorisation should record:

- whether this is the first renewal or on how many occasions it has been renewed
- the same information as outlined for an original application
- details of any significant difference in the information given in the previous authorisation
- the reasons why it is necessary to continue with the surveillance
- the content and value to the investigation or operation of the information so far obtained by the surveillance
- an estimate of the length of time the surveillance will continue to be necessary
- the results of any reviews

1.13 Reviews and Cancellations

The Authorising Officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the surveillance no longer meets the criteria for authorisation. A record should be made of the cancellation and the appropriate form completed.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded. Reviews should be more frequent where there may be collateral surveillance on persons other than those who are the subject of surveillance. In each case the authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

As soon as a decision is taken to cease surveillance, an instruction must be given to those involved in the operation to stop listening, watching or recording the activities of the subject. The date on which that instruction is given should also be recorded.

1.14 Forms

The appropriate forms for authorisation, review, renewal and cancellation of authorisation for DS are annexed as part 3 of this Guidance. All forms will be made available on the intranet.

1.15 The Role of an Authorising Officer

The role of an Authorising Officer (AO) is akin to that of a Magistrate or Judge considering an application to the court for a Warrant or similar. The AO must have all the information he or she feels is necessary to make an independent assessment of the application. The AO should assess, for example: the force of the complaint giving rise to the surveillance, the duration of the surveillance proposed, if recording devices are to be used, an indication of the expected quality should be given. Without examining such issues, an AO will not be able to determine whether the surveillance is both 'necessary' and 'proportionate' and whether, therefore the authorisation should be given. An AO should not hesitate to refuse an application on the grounds of insufficient information. If further details are required, comments may be made on the returned application as to the further information sought.

Criteria to be given Consideration in an application

There are three key elements:

Necessity

To expand on the information given above, the Authorising Officer must be satisfied that the authorisation is *necessary for the purpose of preventing and detecting crime, or preventing disorder*.

The Authorising Officer should refer to sections 28 of RIPA and to the second chapters of the Code of Practice for further guidance as required.

Proportionality

The Authorising Officer must also believe that the surveillance is *proportionate* to what it seeks to achieve – see section 1.16 below.

Collateral Intrusion

An AO must give particular consideration to the potential for “collateral intrusion”. Essentially, this is interference with the privacy of persons other than the subject(s) of surveillance. An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. This will be taken into account by the AO when considering the proportionality of the surveillance. Those carrying out the covert surveillance should inform the AO if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required. The fullest consideration should be given in cases where the subject of the surveillance might reasonably expect a high degree of privacy, for instance in his/her home, or where there are special sensitivities.

1.16 Proportionality

Proportionality is a very important concept, and it means that any interference with a person's rights must be proportionate to the intended objective. This means that the action is aimed at pursuing a legitimate aim (for example, protecting a child from potential abuse). Interference will not be justified if the means used to achieve the aim are excessive in all the circumstances. Thus where surveillance is proposed that action must be designed to do no more than meet the objective in question; it must not be unfair or arbitrary; and the impact on the individual or group of people concerned must not be too severe. The Human Rights Act 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 and is not arbitrary, unfair or based on irrational considerations.

1.17 What records must be kept?

The following records must be kept:

- A copy of the application for the authorisation;
- A copy of the authorisation together with any supplementary documentation and notification of approval given by the authorising officer;
- A record of the period over which the surveillance is taking or has taken place (including any significant suspensions of coverage)
- A record of the frequency and results of periodic reviews of the authorisation
- A copy of any renewal of authorisation, together with the supporting documentation when the renewal was requested
- The date and time when any instruction was given by the authorising officer

IN ADDITION

- A central register of authorisations will be kept in Legal Services. The register will be used to keep track of all BDC's authorisations and record their status. The register may be used for inspection purposes by officers of the OSC. The register must be updated whenever an authorisation is granted, renewed or cancelled. This record should be retained for a period of at least 3 years from the ending of the authorisation and should contain the following information:
 - ┌ the type of the authorisation
 - ┌ the date the authorisation was given
 - ┌ the unique reference number (URN) of the investigation or operation
 - ┌ the title of the investigation or operation, 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 rank/grade of the authorising officer
 - ┌ whether the investigation or operation is likely to result in obtaining confidential information as defined by the Code of Practice
 - ┌ the date the authorisation was cancelled

Where the product of the surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with the established disclosure requirements (e.g. under the Criminal Procedure and Investigations Act 1996) for a suitable further period or until further review.

1.18 Who keeps the records/a central register of authorisations?

Original individual authorisations should be kept by the department carrying out the investigation. Copies of authorisations will be kept by Legal Services together with the Central Register of Authorisations. Copies of the authorisations themselves will be held by Legal for 7 years, according to the Council's Document Retention Policy.

1.19 Breaches of RIPA, its Codes of Practice and the Human Rights Act

The Effect of a RIPA Authorisation

Although it is neither an express statutory requirement nor a stipulation of the Codes of Practice that acts of surveillance carried out by local authorities must be authorised under RIPA, the effect of a RIPA authorisation (correctly completed) is to make the action which is authorised (and the evidence obtained through that action) "lawful for all purposes" (s27(1)). Without such an authorisation, evidence obtained from DS or CHIS may be deemed unlawful and thus be ineffective in any prosecution. In addition, the authority may be exposed to civil or criminal liability for its conduct.

The Effect of the Codes of Practice

Section 72 of RIPA says:

- (1) A person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71 shall, in doing so, have regard to the provisions (so far as they are applicable) of every code of practice for the time being in force under that section.
- (2) A failure on the part of any person to comply with any provision of a code of practice for the time being in force under section 71 shall not of itself render him liable to any criminal or civil proceedings.
- (3) A code of practice in force at any time under section 71 shall be admissible in evidence in any criminal or civil proceedings.
- (4) If any provision of a code of practice issued or revised under section 71 appears to-
 - (a) the court or tribunal conducting any civil or criminal proceedings,
 - (b) the Tribunal,
 - (c) a relevant Commissioner carrying out any of his functions under this Act,
 - (d) a Surveillance Commissioner carrying out his functions under this Act or the Police Act 1997, or
 - (e) any Assistant Surveillance Commissioner carrying out any functions of his under section 63 of this Act,

to be relevant to any question arising in the proceedings, or in connection with the exercise of that jurisdiction or the carrying out of those functions, in relation to a time when it was in force, that provision of the code shall be taken into account in determining that question.

Criminal liability of directors

Section 79 of RIPA says that:

(1) Where an offence under any provision of this Act other than a provision of Part III is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of-

- (a) a director, manager, secretary or other similar officer of the body corporate, or
- (b) any person who was purporting to act in any such capacity,

he (as well as the body corporate) shall be guilty of that offence and liable to be proceeded against and punished accordingly.

Human Rights Act 1998

If covert surveillance or use of a covert human intelligence source is not authorised under RIPA, then the authority will be exposed to the possibility of legal action under the Human Rights Act. The subject of the surveillance may be able to have the evidence obtained in an unauthorised investigation excluded. The articles most likely to be put forward are:

- Article 6 – the right to a fair trial
- Article 8 – the right to respect for private and family life, home and correspondence

Recent Judgments

R v Sutherland [2000] Nottingham Crown Court

This case demonstrates good example of default of the regulations - a murder trial collapsed because an authorisation for directed surveillance had been exceeded.

Martin v United Kingdom [19/92/2004] European Court App 63608/00

There was alleged disorderly behaviour by M towards a neighbour. The local authority mounted UNAUTHORISED covert surveillance of M. M's claim of an article 8 infringement was settled by agreement, with M receiving £4000 damages.

1.20 Obtaining Further Guidance

A full copy of RIPA 2000 can be found online at www.opsi.gov.uk at the following link:
<http://www.legislation.opsi.gov.uk/acts/acts2000/20000023.htm>

The Home Office Codes of Practice on Covert Human Intelligence Sources and Covert Surveillance can be found at the Home Office website: www.homeoffice.gov.uk at the following links:

<http://security.homeoffice.gov.uk/news-and-publications1/publication-search/ripa-cop/covert-cop?view=Standard&pubID=215420> for covert surveillance and at <http://security.homeoffice.gov.uk/news-and-publications1/publication-search/ripa-cop/215443?view=Standard&pubID=215443> for covert human intelligence sources.

The website address for the Office of Surveillance Commissioners is:
<http://surveillancecommissioners.gov.uk>

There is a regularly updated section on judgments in case law.

Forms for authorisation, review, renewal and cancellation of DS are available at:

<http://security.homeoffice.gov.uk/news-and-publications1/publication-search/ripa-cop/215443?view=Standard&pubID=215443>

A copy of the Human Rights Act 1998 can be found online at www.opsi.gov.uk at the following link:
<http://www.legislation.opsi.gov.uk/acts/acts1998/19980042.htm>

GUIDANCE ON AUTHORISATION UNDER RIPA, PART 2 FLOWCHART FOR AUTHORISATION, REVIEW & CANCELLATION PROCEDURE

