

**BABERGH DISTRICT COUNCIL**

**FROM:** Director of Corporate Services

**REPORT NUMBER:** **K107**

**TO:** Council

**DATE OF MEETING:** 28 September 2010

**REVISION OF POLICY CONCERNING THE COUNCIL'S ACTIVITIES UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000**

**1. PURPOSE OF REPORT**

1.1 This report introduces a revised policy which aligns Babergh District Council's existing policy on surveillance activities under the Regulation of Investigatory Powers Act 2000 "RIPA" with the policy of Mid Suffolk District Council to produce a joint corporate policy. The policy also incorporates changes required to be implemented by the coming into force of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (effective 6<sup>th</sup> April 2010) and the revised Codes of Practice issued by the Home Office, which amongst other things, introduce a role for scrutiny committees in the monitoring of activities under RIPA.

**2. RECOMMENDATIONS**

2.1 That the policy attached be adopted subject to any revisions agreed by the Acting Head of Legal Services, Kathryn Saward (Babergh District Council) and the Acting Legal Services Manager, Jonathan Reed (Mid Suffolk District Council).

Council is able to resolve this matter.

**3. FINANCIAL IMPLICATIONS**

None

**4. RISK MANAGEMENT**

4.1 This report is most closely linked with the Council's Significant Business Risk No. 10 (Local Response to National Issues). Key risks are set out below:

<b>Risk Description</b>	<b>Likelihood</b>	<b>Seriousness or Impact</b>	<b>Mitigation Measures</b>
That the steps to be taken to achieve compliance with the 2010 Order will not be reflected in the Council's policy.	Low	Marginal	

Risk Description	Likelihood	Seriousness or Impact	Mitigation Measures
This might cause the Office of the Surveillance Commissioners to give the Council a negative inspection report, on next inspection. (A very negative inspection could ultimately lead to curtailment of the Council's use of RIPA).			

5. **EQUALITY AND DIVERSITY IMPACT**

There are no equality and diversity implications.

6. **KEY INFORMATION**

6.1 Ordinarily, covert surveillance of an individual by a Council would breach that individual's human rights. The provisions of RIPA permit certain law enforcement agencies, including local authorities, to carry out covert surveillance activity without breaching human rights legislation, provided that certain checks and balances on the necessity and proportionality of the activity are thoroughly made by a senior officer within the authority. Records of authorisations and refusals of authorisations must be kept on a central register held by the Council and the authorising officer must record their considerations carefully; the decision being akin to the decision of a magistrate or judge to issue a warrant. Local authorities may carry out surveillance on one ground only; that it is necessary for the prevention or detection of crime or preventing disorder. The covert activity might involve direct surveillance, the use of an agent (known as a covert human intelligence source or 'CHIS') or obtaining details via electronic or telephone communications, known as the 'acquisition of communications data'. In relation to the last type of surveillance local authority is not permitted to access the contents of such communications, only peripheral information such as numbers or addresses used, or the frequency of calls. The records kept by the local authority are subject to regular inspection by the Office of the Surveillance Commissioner, and statistics on authorisations are returned annually.

6.2 The report introduces the following measures to Babergh's policy:

- a role for Scrutiny Committee in regularly monitoring policy, practice and procedure;
- the role of "Senior Responsible Officer" which again involves monitoring and oversight of the Council's RIPA activities together with responsibility for implementation of policy and engagement with the Office of the Surveillance Commissioner;

- the concept of the acquisition of communications data (to date the Council has not made any request for the acquisition of communications data, although such powers have been available);
- a Single Point of Contact (“SPoC”) for requests for the acquisition of communications data. The SPoC is required to be an accredited person. Mid Suffolk District Council had an accredited SPoC in place and have offered that Babergh may adopt that person as its SPoC.

7. **APPENDICES**

Draft Joint Corporate Policy and Procedures under the Regulation of Investigatory Powers Act 2000

8. **BACKGROUND PAPERS REFERRED TO:**

None

**CONTACT:** Caroline Whatling  
Legal Services

**EMAIL:** [caroline.whatling@babergh.gov.uk](mailto:caroline.whatling@babergh.gov.uk)

BABERGH DISTRICT COUNCIL  
AND  
MID SUFFOLK DISTRICT COUNCIL  
JOINT CORPORATE POLICY  
& PROCEDURES  
THE REGULATION OF INVESTIGATORY  
POWERS ACT 2000  
(‘RIPA’)

## CONTENTS

1. Introduction
2. Recent Legal Developments
- 3.1 Policy Statement – General
- 3.2. Policy Statement on Surveillance
- 3.3. Policy Statement on Communications Data
4. Guidance and Procedures for Officers
  - 4.1 Surveillance under RIPA
  - 4.2 RIPA PART II (Directed Surveillance)
  - 4.3 RIPA PART II (Covert Human Intelligence Sources)
  - 4.4 RIPA PART I CHAPTER II (Communications Data)
  - 4.5 Authorisation Procedures and Authorising Officers
  - 4.6 Guidance for Authorising Officers
5. What Records Must Be Kept?
6. Breaches of RIPA
7. Where to Find Further Information

### APPENDICES (refer to section 7 for where to find these documents online)

#### (i) FORMS

##### Directed Surveillance

- A - Application for Authorisation to carry out Directed Surveillance
- B - Review of a Directed Surveillance Authorisation
- C - Cancellation of a Directed Surveillance Authorisation
- D - Application for Renewal of a Directed Surveillance Authorisation

##### Communications Data

- E - Notice under Section 22(4) of RIPA requiring Communications Data to be obtained and disclosed (Part I Chapter II Notice)
- F - Application for Communications Data
- G - Designated Person's consideration form in respect of an application for Communications Data.

#### (ii) CODES OF PRACTICE

- H - Code of Practice for Covert Surveillance and Property Interference
- I - Code of Practice for the Use of Covert Human Intelligence Sources
- J - Code of Practice on the Acquisition and Disclosure of Communications Data

## **1. Introduction**

The Regulation of Investigatory Powers Act 2000 is probably better known by its acronym "RIPA". It addresses human rights issues arising from the carrying out of surveillance and the accessing of communications data by local authorities and other law enforcement agencies. The legislation and its codes of practice set out a framework to justify that in certain circumstances, such activity is in accordance with the law, where it might otherwise be contrary to Human Rights legislation.

*There is no legal requirement to obtain an authorisation under RIPA.* In that sense it is a 'voluntary' system. However, if the subject of surveillance were to challenge the surveillance-based evidence in a case brought by the enforcing agency, or were to make a stand-alone challenge to the way the surveillance was carried out, it might be hard to justify that such activity was in accordance with the law without a RIPA authorization.

So, failure to follow the procedures contained within RIPA and its codes *may* render any evidence gathered inadmissible and/or *may* result in a breach of an individual's human rights.

Under Article 8 of The Human Rights Act 1998, public authorities must respect an individual's "right to respect for his private and family life, his home and his correspondence". This right is not absolute, and is qualified thus: -

***"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."***

Any such interference with the right under Article 8 must be:

- lawful
- necessary and
- proportionate.

RIPA provides a statutory mechanism for the internal authorisation of:

- covert 'directed' surveillance
- covert use of a 'human intelligence source' and
- access to communications data.

This policy document gives an overview of the parts of the Act relevant to Mid Suffolk and Babergh District Councils (and CSD as an agent for MSDC) ("the Councils") and explains the procedures to be followed. Appropriate training will be organised at regular intervals and is compulsory both for those officers identified by their Heads of Service as being involved in enforcement work and for Authorising Officers. Various departments may need to carry out surveillance in order to prevent or detect crime. These include the following service areas : -

Audit & Fraud Investigation (including Benefit/Housing Fraud)  
Food Safety  
Planning Enforcement  
Environmental Services  
Waste Management  
Licensing  
Housing & Community Development

This policy will be regularly reviewed, by the Senior Responsible Officers, by the RIPA Working Group and by Scrutiny Committee in relation to legal development and for the purpose of monitoring and oversight of practice and procedure.

## **2. Recent Legal Developments**

The use of RIPA has recently come to public attention because local authorities had used RIPA authorisations to investigate such matters as fraud relating to school catchment areas, dog fouling and people putting their bins out too early. (The first of these has since been found not to be a proper purpose for RIPA powers by the Investigatory Powers Tribunal). Such authorisations were regarded by press and public as an inappropriate use of RIPA powers, and it was mooted that such powers were appropriate only for anti-terrorism activities or serious crime. As a result the government carried out an extensive consultation, which led to the introduction of revised Codes of Practice and Consolidating Orders, which came into force on 6<sup>th</sup> April 2010. The publication "Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice, A Public Consultation Paper" had made it clear that it was the government's intention to curb the RIPA powers previously held by local authorities.

The most significant practical change under of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 is that the seniority of Authorising Officers is raised to Director/Head of Service/Service Manager or above.

Under the revised Codes of Practice the following changes are necessary:

- oversight is to be increased by adding Councillors to the process. Councillors (i.e. Scrutiny Committee) should review the authority's use of RIPA and set the policy at least once a year. They should also consider internal reports on the use of RIPA at least on a quarterly basis to ensure that it is being used consistently with the council's policy and that the policy remains fit for purpose.
- a Senior Responsible Officer ("SRO") is to be made responsible for the integrity of process for the management of Directed Surveillance and Covert Human Intelligence Sources, for compliance with Part 2 of the Act and its Codes; for oversight of the reporting of errors to the Commissioner; for engagement with OSC Inspectors; and for the implementation of post-inspection action plans approved by a Commissioner. For Babergh District Council the SRO will be the Acting Head of Legal Services. For Mid Suffolk District Council the SRO will be Acting Legal Services Manager.

The Codes are also intended to provide greater clarity on:

- i) when the use of RIPA techniques is likely to be proportionate;
- ii) when public authorities do/do not need to use RIPA authorisations; and

- iii) collateral intrusion.

The intended objective is that with increased and intensified monitoring activity, the balance between supporting law enforcement and respecting privacy will be more effectively achieved.

It remains a possibility that the authorising powers held by local authorities may in future be removed to the magistrates' court, so that an authorisation would need to be sought in the same way as a warrant. Other possible adjustment might include the limitation of RIPA powers to "serious" crime as defined by the type of conduct (e.g. violence/substantial financial gain) or the possible sentence (e.g. three years or more). This would exclude most local authority enforcement.

### **3. General Policy Statement - Steps Taken to Achieve Compliance**

A forum comprising legal advisers, authorising officers and operational staff known as the 'RIPA Working Group' meets regularly to monitor procedure and performance and note any developments in the law.

The Councils have agreed for the present to implement Directed Surveillance ("DS") only and not to use Covert Human Intelligence Sources ("CHIS") which carries greater risk and is more complex. This policy is to be kept under review based on the need for CHIS within the Councils. There has not previously been a significant demand for use of CHIS. The RIPA Working Group, the SROs and Scrutiny Committee will regularly review the need for CHIS, which requires specialist training for the relevant officer.

The Councils will only use DS as a last resort. Wherever practicable, the Councils 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.

The Councils have produced guidance on DS for officers which forms part of this document. The guidance on CHIS is limited to enable officers and members to identify what constitutes CHIS and very broadly, what authorisation would involve.

Central Registers of RIPA authorisations for both Councils are held by Legal Services together with copies of authorisations given. The Councils have nominated the Acting Head of Legal Services (for Babergh DC) and the Acting Legal Services Manager (for Mid Suffolk DC) as being the Senior Responsible Officers whose role is to ensure the proper administration and adoption of relevant procedures.

The Scrutiny Committees of both Councils will regularly monitor policy, practice and procedure.

An accredited Single Point of Contact is in place to handle requests for the acquisition of communications data.

The Councils will ensure that records pertaining to DS and the acquisition of communications data are retained, according to their Document Retention Policies, for a minimum of 7 years.

### **3.2 Policy Statement on Surveillance – RIPA Part II**

The Councils will ensure that all surveillance undertaken by officers will be conducted in accordance with the Codes of Practice issued by the Home Office and practical advice from the Office of the Surveillance Commissioner (OSC). By adopting this approach the Councils are endeavouring to ensure that there are no breaches of the Human Rights Act 1998 or of the Regulation of Investigatory Powers Act 2000 itself. The implications of not observing the legislation, 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 Councils conduct themselves in investigatory activities (e.g. possible abuse of statutory powers) leading to a general loss of confidence
- possibility of increased complaints and compensation claims to the Councils
- 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 Councils under the Human Rights Act.

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

### **3.3. Policy Statement on Access to Communications Data - RIPA Part I Chapter II**

At the date of writing this policy, the Councils have not needed to access Communications Data. However, the requirements of Part I of the Act remain in place, and the Councils must be in a state of preparedness should the need arise.

This part of the Act gives public authorities the power to acquire communications data. It covers any conduct in relation to a postal service or telecommunication system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself, i.e. contents of e-mails or interactions with websites.

Part I introduces a statutory framework to regulate access to communications data by public authorities consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, reflecting the requirement of Article 8:

***“There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”***

As in Part II, any such interference must be: -

- lawful
- necessary
- proportionate

AND any such authorisations for access to communications data may only be granted if the Authorising Officer believes that such authorisation is necessary for the prevention or detection of crime or preventing disorder.

All authorisations, reviews, cancellations and rejections will be filed in the central register held in each organisation. All must be completed using the correct, current version of the RIPA forms.

Certain safeguards apply to public authorities accessing Communications Data under RIPA.

1. The persons designated to seek access to data must be clearly specified.
2. There is an accreditation scheme for certain individuals with access to such data
3. There must be compliance with the statutory Codes of Practice.
4. The Interception of Communications Commissioner is responsible for overseeing all requests for data.
5. There are sanctions available for abuse of powers to access communications data.

## Guidance and Procedure for Officers

### 4.1 RIPA Part II - Surveillance

#### Overt Surveillance does not require authorisation under RIPA

Overt surveillance is, as its name would suggest, surveillance which is open. In other words, there is nothing secretive or hidden about it. Officers may carry out overt surveillance in the course of a normal day's work, and this does not require any prior authorisation.

#### Covert Surveillance requires authorisation under RIPA

Part II of the Act identifies three categories of covert (i.e. secret or hidden) activity which may be authorised if the correct procedure is followed and the established criteria are met. These are:

- i) Intrusive Surveillance (this category may not be authorised by a local authority)
- ii) Directed Surveillance
- iii) Covert Human Intelligence Sources

### Intrusive Surveillance

A local authority may not authorise Intrusive Surveillance and the Councils therefore **may not** carry out intrusive surveillance under any circumstances. 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. Authorisation may 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.

### 4.2 Directed Surveillance (“DS”)

This is:

- **covert** but *not intrusive* (see below) surveillance, which is
- undertaken for a **specific** investigation or operation (not as an immediate response to events or as part of a routine patrol) and
- 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. The glossary to the Covert Surveillance Code of Practice defines private information as:

*“Any information relating to a person in relation to which that person has or may have a reasonable expectation of privacy. This includes information relating to a person’s private, family or professional affairs. Private information includes information about any person, not just the subject(s) of the investigation”* and also (at para 2.4) says it should be taken to include

*“...any aspect of a person’s private or personal relationship with others, including family and professional or business relationships.”* It goes on to say that this can include personal data such as names, telephone numbers and addresses and that “family should be treated as extending beyond the formal relationships created by marriage or civil partnerships. E.g. a person observed running a commercial baking business from her home became subject to investigation. Such an investigation should be subject to

the RIPA consideration/authorisation process as any surveillance could result in obtaining private information about her. Case law demonstrates that breaches of Article 8 can occur even in a public place (see the case of Peck -v- UK) and also that private life is widely interpreted by the courts, covering activities which take place at business premises. In the case of Ammam –v- Switzerland the court said “*Respect for private life comprises the right to establish and develop relations with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of “private life” should be taken to exclude activities of a professional or business nature.*”

### How can Directed Surveillance be authorised?

The Act says that DS can be authorised by a "designated person". A list of designated people at the Councils can be found below in the section 5.5 entitled ‘Authorising Officers’.

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.

### 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 has not been notified in advance (NB – advance “warning letter” are valid for a period of up to 4 weeks maximum) of potential surveillance
- 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 still camera or video recording equipment 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.

#### Use of Technical Equipment

Covert surveillance 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 would require authorisation.

#### 4.3 Covert Human Intelligence Sources (CHIS)

The Councils will not authorise CHIS at present, but the need for CHIS will be kept under review. The guidance in this section should enable officers and councillors to identify what would constitute 'CHIS'.

This type of surveillance involves 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, the Councils no longer authorise CHIS. However, in order that Council 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.

### Authorisation of CHIS

Two elements need to be authorised with a CHIS: -

- Conduct – establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.
- Use – actions inducing, asking or assisting a person to act as a CHIS and the initial decision to use a CHIS

Special rules apply to juveniles and vulnerable people.

## 4.4 RIPA PART I CHAPTER II (Communications Data)

### Categories of Communications Data

There are three broad areas of communications data, only two of which can be accessed by the Councils. They are as follows:

1. Section 21(4)(c) Information about Communications Service users, such as:
  - Name of account holder/subscriber
  - Installation and billing addresses
  - Method of payment/ billing arrangements
  - Collection/delivery arrangements for a PO Box (i.e. whether it is collected or delivered – not where it is collected from or delivered to)
  - Other customer information e.g. account notes, demographic information or sign up data (not passwords or personalised access information)
2. Section 21(4)(b) Information about the use of communications services
  - Outgoing calls on a landline telephone or contract or prepay mobile phone
  - Timing and duration of service usage
  - Itemized connection records
  - Internet logon history
  - E-mails (sent)
  - Information about the connection, disconnection and reconnection of services
  - Information about the provision of conference calling, call messaging, call waiting and call barring
  - Information about the provision and use of forwarding/redirection services (postal and telecom)
  - Records of postal items e.g. records of registered/recorded/special delivery postal item, records of parcel consignment/delivery/collection

### Organisations from which the Councils may access Communications Data

All Communications Data is accessed from Communication Service Providers (CSPs). These may be:

- **Telecom providers,**  
mobile phone service providers, landline phone service providers or International Simple Voice Resellers
- **Internet Providers**  
ISPs, Virtual ISPs and Portals
- **Postal Providers**  
Postal services

#### Applying for an Authorisation to Obtain Communications Data

Application must be made using the appropriate form. It must include the following information:

- Name or designation of the officer requesting the communications data
- The operation and person (if known) to which the requested data relates
- A description of the data requested
- Identification which section of the Act the communications data is covered by
- Reasons why obtaining the data is considered to be necessary under Section 22(2) of the Act. **N.B. there is only one reason - for the prevention or detection of crime or preventing disorder.**
- An explanation as to why obtaining the data is proportionate to what it seeks to achieve
- An indication (where appropriate) that the matter of collateral intrusion has been considered.

Application forms are subject to inspection by the Interception of Communications Commissioner. Both the applicant and the Designated Person may be required to justify any decisions they have made.

All notices and Authorisations for Communications Data must be channelled through a “Single Point of Contact” (SPoC) who must be approved by the Home Office, and who must have received the appropriate training.

This system aims to provide an efficient regime, as the SPoC will deal with the postal or telecommunications operator on a regular basis, the Councils will be able to regulate themselves, and it will help reduce the burden on the postal and telecommunications operator.

The SPoC for both Councils is Mr David Abbott, an Enforcement Officer based at Mid Suffolk District Council.

#### Responsibilities and Role of the Single Point of Contact (“SPoC”)

Notices and authorisations should be passed through the SPoC. The SPoC should be in a position to:

- Where appropriate, assess whether access to communication data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and Designated Person on whether communications data falls under section 21(4)(a), (b) or (c) of the Act;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the postal or telecommunications operator.

The SPoC must have received the appropriate training and have passed an exam before being approved by the Home Office. The SPoC must keep abreast of the law relating to, and developments within, the communications industry.

The SPoC has the following duties:

- to assess whether access to communications data in a particular case is reasonably practical for the CSP
- to advise investigators and Designated Persons on the practicalities of accessing different types of communications data from different CSPs.
- to advise investigators and Designated Persons on whether specific communications data falls under Section 21(4)(b) or 21(4)(c) of RIPA.
- to assess any cost and resource implications for both the Council and the CSP
- to provide a safeguard for CSPs that authorisations and notices are authentic.
- to retain records of all applications, Authorisations and Notices
- to retain a record of the dates on which Authorisations and Notices are started and cancelled.
- to retain all Applications in the event that there may be a complaints Tribunal.
- to retain a record of any errors that may have occurred in the granting of Authorisations, or issuing of notices, and provide an explanation to the Interception of Communications Commissioner.

### Ways of obtaining Communications Data

Under RIPA, there are two permissible ways of accessing Communications Data.

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

A Notice is where a CSP collects data on behalf of the Council. The form of Notice must include the following information:

- A description of the data required (and whether it is Communications Data under Section 21(4)(b) or Section 21(4)(c) of the Act.
- The purpose for which the data is required. **This will always be for the prevention or detection of crime or preventing disorder.**
- The name (or designation) and office, rank or position of the Designated Person
- The manner in which the data should be disclosed
- A unique reference number
- If relevant, any indication of urgency
- A statement setting out that data is sought under the provisions of Part I, Chapter II of the Act
- Contact details

## 2. Authorisation under Section 22(3)

A section 22(3) authorisation is used by the Council collecting or retrieving the Communications Data itself. It may only be given in these circumstances:

- When the Postal or Telecommunications operator is not capable of obtaining or retrieving the communications data
- When it is believed that the investigation may be prejudiced if the Postal or Telecommunications Operator is asked to collect the data itself
- When there is a prior agreement in place between the Council and the Postal or Telecommunications Operator as to the appropriate mechanisms for the disclosure of Communications Data

Each Authorisation must include the following information:

- A description of the conduct that is authorised
- A description of the Communications Data required (identify whether it is Communications Data under Section 21(4)(b) or 21(4)(c) of the Act)
- Identify the purpose for which the data is required. **This will always be for the prevention or detection of crime or preventing disorder.**
- The name (or designation) and office, rank or position of the Designated Person
- A unique reference number

Authorisations and notices are valid for one month, but can be renewed using the appropriate form. They must be cancelled as soon as they are no longer considered to be either necessary or proportionate.

It is the duty of a Designated Person to cancel Authorisations and Notices.

### Designated Persons (Authorising Officers) and their Responsibilities

An Authorising Officer for Communications Data must be a Head of Service or above.

Authorising Officers must ensure that requests for Communications Data are both necessary and proportionate prior to granting an Authorisation or issuing a Notice.

They have a duty to consider various points, as follows:

- Whether the case justifies the accessing of Communications Data under Section 22(2)(b) i.e. that it is for the prevention or detection of crime or preventing disorder.
- Whether obtaining access to the data by the conduct authorized by eh authorisation, or required of the CSP in the case of a Notice, is proportionate to what is sought to be achieved
- Whether the circumstances of the case still justify such access in cases where there is likely to be collateral intrusion
- Whether any urgent time scale is justified.

N.B. Communications data cannot be used in evidence without it being produced in a statement by the CSP involved.

#### **4.4 AUTHORISATION PROCEDURE AND AUTHORISING OFFICERS FOR RIPA PARTS I AND II**

##### a) Authorisation procedures

Prior authorisation for directed surveillance or for use of a covert human intelligence source needs to be obtained from an Authorising Officer. All authorisations, reviews, cancellations and rejections will be filed in a central register kept in the Legal Services section of both Councils. All must be completed using the correct, current version of the RIPA forms.

##### 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.

#### b) Duration of Authorisations

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.

#### c) 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

#### d) 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.

#### e) Authorising Officers

The following are Authorising Officers for the purposes of Parts I and II of RIPA: -

#### Babergh District Council

Chief Executive  
Deputy Chief Executive  
Head of Natural & Built Environment  
Director of Finance

#### Mid Suffolk District Council

Chief Executive  
Corporate Directors x 2  
Planning Control Manager  
Environmental Health Officer  
Housing Services Manager  
Waste & Environmental Services Manager

#### CSD staff

Benefits Manager  
Revenues Manager

Authorisations may only be given to an organisation by its own Authorising Officers. Authorising Officers should not give authorisations relating to their own service, e.g. the Planning Control Manager should not authorise surveillance for a planning enforcement matter.

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:

the Chief Executive , or in her/his absence only the Deputy Chief Executive at Babergh DC or a Corporate Director at MSDC.

#### 4.6 Guidance for Authorising Officers

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 she or he 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.

Application forms are subject to inspection by the Surveillance Commissioner. Both the applicant and the Authorising Officer may be required to justify any decisions they have made.

The primary consideration for an Authorising Officer is that authorisations for directed surveillance may only be granted if the Authorising Officer is certain that such authorisation is necessary **for the prevention or detection of crime or preventing disorder**.

Before signing an authorisation, an Authorising Officer needs to be satisfied that the authorisation is: -

- in accordance with the law
- necessary (consider - is there reasonably available another, overt, means of discovering the information desired?)
- proportionate (consider – is the proposed surveillance the **least intrusive** method available? Is it **excessive** in relation to the seriousness of what is being investigated? The Authorising Officer should be satisfied, prior to authorisation, that all other avenues for obtaining the necessary evidence have been explored.

The likelihood of “collateral intrusion” must also be considered. The Authorising Officer should ensure that intrusion to individuals who are not the intended subject of the investigation is avoided or at least minimised.

If the period of authorisation is not made clear on the authorisation form, then an authorisation will be effective for a period of three months, after which it ceases to have effect (unless renewed in the meantime). Reviews should be carried out periodically, to ensure that the authorisation continues to meet the criteria. If it does not, it should be cancelled using the appropriate form (please see forms attached). Even those authorisations where the time period is specified need to be cancelled using a cancellation form.

#### Further Guidance on Criteria to be given Consideration in an application

##### 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.

### 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.

### **5. 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 the Councils' 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.

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

Copies of individual authorisations should be kept by the department carrying out the investigation. The original authorisations will be kept by Legal Services together with the Central Register of Authorisations. Copies of the authorisations themselves will be held by Legal Services for 7 years, according to the Council's Document Retention Policy. Any copy authorisations held by individual departments should be destroyed according to the retention policy for that type of file.

### **6. 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

## **7. Where to find further information**

The web address for the Office of the Surveillance Commissioners is:

<http://www.surveillancecommissioners.gov.uk/>

A full copy of RIPA 2000 can be found at:

<http://www.legislation.gov.uk/ukpga/2000/23/contents>

Orders relating to RIPA can be found at

[http://www.surveillancecommissioners.gov.uk/advice\\_acts.html](http://www.surveillancecommissioners.gov.uk/advice_acts.html)

The Codes of Practice can be found at:

<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/>

RIPA forms can be found at:

<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/>

A copy of the Human Rights Act 1998 can be found at:

<http://www.legislation.gov.uk/ukpga/1998/42/contents>

Useful sites for information about human rights are:

[http://www.direct.gov.uk/en/Governmentcitizensandrights/Yourrightsandresponsibilities/DG\\_4002951](http://www.direct.gov.uk/en/Governmentcitizensandrights/Yourrightsandresponsibilities/DG_4002951)

<http://www.yourrights.org.uk/>

<http://www.justice.gov.uk/about/human-rights.htm>

Forms for authorisation, review, renewal and cancellation can be found at:

(NB - Councils have their own tailored versions of the forms)

<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/>

A useful website for information on and discussion of the latest developments is:

<http://www.actnow.org.uk/content/10>

H:\DOCS\Committee\REPORTS\COUNCIL\2010\280910-JOINT RIPA POLICY.doc