

**SWINDON BOROUGH COUNCIL**

**POLICY & PROTOCOL ON**

**REGULATION OF INVESTIGATORY**

**POWERS ACT 2000**

Scope

This Protocol applies to authorisations for surveillance (not involving entry on or interference with property or wireless telegraphy as regulated by the Police Act 1997); the use of covert human intelligence sources and the acquisition of communication data – Local Authority Investigation Sections.

# 1. INTRODUCTION

## 1.1 Background

1.1.1 The Human Rights Act 1998 (HRA) was introduced to give effect to European Convention on Human Rights (ECHR) and came into force in October 2000. From that date the ECHR became part of our domestic law. Consequently, individuals may enforce their rights under ECHR in domestic courts rather than having to go before the European Court of Human Rights in Strasbourg.

1.1.2 The HRA imposes a duty upon the Council to act in a way that is compatible with the rights under ECHR. Failure to do so may enable a person to seek damages against the Council or to use our failure as a defence in any proceedings that we may bring against them.

## 1.2 European Convention on Human Rights (ECHR)

1.2.1 Under Article 6 of the ECHR, everyone is entitled to a fair and public hearing, within a reasonable time, of any criminal charge against him or her or into the determination of any civil dispute.

1.2.2 Under Article 8, everyone also has the right to respect for the private and family life, their home and their correspondence. The Article recognises that there may be circumstances in a democratic society where it may be necessary for the State (which includes the Council) to interfere with this right. This can only be done in accordance with the law and for clearly defined purposes. These purposes are: -

- In the interest of national security;
- In the interest of public safety;
- In the interest of the economic well-being of the country;
- For the prevention or detection of crime or of preventing disorder;
- The protection of health or morals;
- For the purposes of assessing or collecting any tax, levy or other imposition, contribution or charge payable to a government department;
- For the purpose, in emergency, of preventing death or injury or any damage to a person's physical or mental health, or mitigating the same;
- For any other purpose as specified by the Secretary of State.

**Local Authorities can only carry out surveillance for the purpose of the prevention or detection of crime or of preventing disorder.**

## 1.3 Impact on Investigations

1.3.1 To be able to justify any interference with the right to respect for an individual's privacy, and comply with the HRA, the Council will need to

demonstrate that any intrusion into an individual's privacy is necessary for the purposes of an investigation. Surveillance is often a necessary part of any investigation. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of covert surveillance and the acquisition of communication data. Where it is considered appropriate, it will be necessary for it to be authorised before it can commence. This applies where the surveillance is being undertaken by the Council Officers or by an outside agency acting on the Council's behalf. Authorising officers will need to satisfy themselves that a defensible case can be made for covert surveillance activity.

1.3.2 The Secretary of State has issued codes of practice on the use of covert surveillance under RIPA. The codes are admissible as evidence in criminal and civil proceedings. A court or tribunal must take any relevant provision of the codes into account.

## 1.4 Policy and Codes of Guidance

1.4.1 To ensure that authorisations and procedures are applied in a consistent way, the Council has adopted a policy covering the authorisation, the use of covert surveillance and the acquisition of communication data, as well as approving a Protocol.

1.4.2 This document is in four parts: -

- The Council's Policy on the Use of Surveillance and the acquisition of communication data.
- Easy Reference Guide to the Code of Practice and Procedure;
- Forms
- The codes of practice.

1.4.3 The Statutory Codes of Practice are incorporated as **Appendix C**. In cases of conflict between the Policy, the Easy Reference Guide and the Statutory Codes of Practice, the latter shall prevail.

1.4.4 The Council adopted the Policy and Code of Guidance on the 25<sup>th</sup> September 2002 and has been subsequently revised. This revision was issued in March 2007

## **PART 1 – STATEMENT OF POLICY**

1. The Council and officers, as well as those acting on its behalf undertaking investigations into criminal offences and breaches of the civil law will endeavour to comply with the following statement of policy at all times.

*In carrying out investigations into criminal offences and breaches of the civil law, the Council will seek to ensure that any interference with the rights of any person is in accordance with the law and is justified by reason of it being undertaken for a legitimate purpose. The use of the covert surveillance or the acquisition of communication data will be conducted in accordance with the statutory code of practice then in force. The means to be employed in any investigation will be proportionate.*

*Proportionate is an essential element of the Human Rights Act; in order to be proportionate any surveillance must not be arbitrary, unfair or excessive. The extent of the surveillance must be balanced against the individual's human rights. Other less intrusive methods must be considered first, as must the need for the information and the purpose for which the information is sought. Surveillance must not be used for marginal benefits or trivial cases.*

## **PART 2 – EASY REFERENCE GUIDE TO PROCEDURES AND THE CODES OF PRACTICE**

### **2.1 Introduction**

2.1.1 This Easy Reference Guide seeks to set out the Council’s procedures for the authorisation of surveillance operations and acquisitions of communications data, and to provide a brief summary of the main points in the Statutory Codes of Practice on Covert Surveillance. The Statutory Codes of Practice are set out at **Appendix C**. The SWERCOTS Enforcement Manual details the procedures, which must be followed when conducting surveillance operations, acting or using a Covert Human Intelligence Source or seeking communications data. This manual is available through Trading Standards Service. Where the Council’s CCTV is used for surveillance purposes the CCTV manual must be followed, this is located in the CCTV control room.

2.1.2 This guidance is an aide for clarification and is **not** a substitute for the Codes themselves.

### **2.2 Surveillance**

2.2.1 Surveillance includes monitoring, observation or listening to persons, their movements, their conversations or their other activities or communications. If surveillance is carried out without the person’s knowledge, it will be covert and require prior authorisation.

2.2.2 RIPA applies to “directed surveillance”, “intrusive surveillance” and the use of “covert human intelligence sources”.

### **2.3 What is “Directed Surveillance”?**

2.3.1 Surveillance will be “directed surveillance” if:

- It is covert;
- Undertaken for a specific operation; and
- Is carried out in such a way as to make it more likely that private information will be obtained about a person.

2.3.2 “Private Information” includes any information relating to a person’s private and family life. This phrase echoes that of Article 8 of the ECHR and should therefore be considered to include questions of personal and sexual identity, personal information, telephone calls from business premises, health and injury and sexual activity.

2.3.3 Directed surveillance excludes intrusive surveillance, which is surveillance carried out on residential premises or in any private vehicle where the observer is present in the premises or vehicle, or is

carried out using a surveillance device. The Council is not permitted to carry out intrusive surveillance.

## 2.4 “Covert Human Intelligence Sources”

### 2.4.1 What is a Covert Human Intelligence Source (CHIS)?

A person is a Covert Human Intelligence Source if:

- (a) The source establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) and (c) below.
- (b) The source covertly uses such a relationship to obtain information or provide access to any information to another person; or
- (c) The source covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

### 2.4.2 Examples of Covert Human Intelligence Sources.

- (i) Purchases from a person selling goods from home should be covered by a CHIS Authorisation, both because the nature of discussion generally might go further than an across-the-counter exchange and to avoid intrusive surveillance.
- (ii) Trading Standards Officers may use residential and business premises, rented specifically for the purpose, to invite suspected rogue traders to quote for business. Even if residential premises are used, officers are not living there so it could be argued that it is not intrusive surveillance. A CHIS Authorisation should be used. However if hidden cameras are used on the premises then this may be intrusive surveillance.
- (iii) An officer working under cover, gathering information by concealing his or her identity will usually require the activity to be authorised, in accordance with the forms in Appendix A. The authorisation would also cover the use of any body worn covert recording device. Other directed surveillance of a covert human intelligence source would require separate authorisation.
- (iv) Routine test purchases where the officer acts as a member of the public and purchases goods for sale **will not** require authorisation. If the officer extends this situation in any significant way, by for example,

- Engaging the seller in conversation to elicit information;
- Developing a relationship with the seller to gain access to goods not on display.

Then authorisation will be required for the use of a covert human intelligence source.

2.4.3 If officers are considering the use of a CHIS they must seek advice and guidance from the Legal Services Department, prior to completing the RIPA application. If

2.4.4 Where the authority uses a CHIS, that CHIS should be assigned a “handler”, the “handler” will keep regular contact with the CHIS, or daily where the Authority uses one of its own officers as the CHIS. The handler will ensure that the CHIS’ identify has not been compromised and will destroy all records which identify the CHIS once the investigation has been completed.

2.4.5 The authority shall also appoint a ‘Controller’ who will have general oversight of the use made of the source.

2.4.6 Before a CHIS is used a risk assessment must be completed and kept with the application **Form RIPA10**. This risk assessment should be reviewed at least monthly.

## **2.5 Is the surveillance permitted and does it require authorisation?**

2.5.1 The processes and procedures outlined in the Codes of Practice are shown diagrammatically in **Table 1**.

## **2.6 Completion of Risk Assessments**

2.6.1 Where a request for surveillance is requested, the Authorising Officer will also have to be satisfied that the risks of collateral intrusion have been properly considered. Collateral intrusion is where a third party’s privacy is being infringed. For example, where an officer takes still or video photographs, or observes one or more innocent third parties, this could be considered as being collateral intrusion. If in the course of investigating a case, a third party’s privacy has been inadvertently invaded, the action should be defensible from a legal viewpoint, provided that the grounds for investigation are sound, i.e. the investigation has been undertaken to detect and/or prevent fraud or some other offence for which the Council is the enforcing authority and the actions are reasonable.

2.6.2 Accordingly, Investigating Officers may need to identify whether a location is suitable for surveillance, for example, by “drive-by’s”. This is

not prevented under the Code of Practice. However if officers make more than one “drive-by” then authorisation may be required. It is possible to complete more than one “drive-by” without an authorisation, for example, where the officer’s observation was interrupted or blocked in some way.

## 2.7 Written Authorisation

2.7.1 Unless a warning letter has been sent to an individual advising them that a complaint has been received and informing them that monitoring of a type described in the letter will be undertaken, before surveillance can be carried out, the Investigating Officer must:

- Complete an application for authorisation to use surveillance on **Form RIPA1**; and for CHIS, **Form RIPA10**.
- Obtain authorisation from an Authorised Officer. Appendix B lists the officer’s the Council has designed as being able to authorise surveillance

2.7.2 Warning letters must identify the period during which any surveillance will take place, a maximum of 12 months. This should be reviewed on at least a monthly basis. A copy of the warning letter should be kept with the application for authorisation to use surveillance.

## 2.8 Time Limit on Written Authorisation

2.8.1 Written authorisation is valid for a maximum of three months, and must be reviewed by the Authorising Officer at least **every** month. If it is necessary to continue the surveillance for longer than three months or in the case of a CHIS one year, an application for a renewal of authorisation for surveillance must be made on **Form RIPA 2** or CHIS **Form RIPA 12**. The Authorising Officer, after carrying out a review, should complete **Form RIPA 4** or CHIS **Form RIPA 11**.

## 2.9 Time Limit on Oral Authorisation

2.9.1 If urgent surveillance is required, oral authorisation can be given but the Authorising Officer must complete **Form RIPA 1** or for CHIS **Form RIPA 10**. Oral authorisation is for use where, the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to jeopardise the investigation or operation.

2.9.2 Oral authorisation may only apply for 72 hours from the time given. If the surveillance is required to continue past that period, written authorisation must be sought.

- 2.9.3 Where oral authorisation has been given the investigating officer must record the detail of the surveillance authorised by the Authorising officer in their official notebook.

## **2.10 Cancellation of Authorisation of Surveillance**

- 2.10.1 At the end of any surveillance that has been carried out, the Authorising Officer must complete **Form RIPA 3** (or CHIS **Form RIPA 13**) to cancel the authorisation for surveillance, in addition a review should also take place.

- 2.10.2 The officer is responsible for the proper storage of any products of the surveillance. All information and materials must be stored securely and an audit log kept of what has been collected and where it is stored. Any information that is not required as evidence should be destroyed as soon as practicable and any product of collateral intrusion must be destroyed as soon as possible.

## **2.11 When Authorisation of Surveillance In or Into a Public Place is Not Required**

- 2.11.1 Where the use of CCTV surveillance systems (fixed or mobile) is overt, usually by way of a notice, authorisation is not required. However if the camera is used to observe the actions of a particular individual then the surveillance becomes directed and covert, therefore an authorisation would be required.

- 2.11.2 Where a person suspected of having committed an offence has been notified that his activities are being monitored, no authorisation will be required. For example, where the Council receives a noise complaint, or it is alleged that goods are being displayed on the highway verge, if a letter is sent to the person responsible for the alleged nuisance or display, notifying him that the level of noise from his premises or activities are being monitored, any surveillance will not be covert. However any recording of conversations, rather than just the level of noise is intrusive surveillance and must not be done. However the investigating officer must consider whether there is likely to be any collateral intrusion as a result of his surveillance. If there is any likelihood of any collateral intrusion an authorisation will be required.

## **2.12 Surveillance where it is likely that Confidential Material will be obtained**

- 2.12.1 If, exceptionally, an Investigating Officer thinks that in the course of conducting surveillance he may obtain confidential information, the Investigating Officer will have to obtain authorisation from the Chief Executive as outlined in 2.6.1 on **Form RIPA 1**. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

- Legal privilege includes communications between a professional legal adviser and his client or any person representing his client, which are made in connection with the giving of legal advice to the client or between a professional legal adviser and his client or any person representing his client, or between a professional legal adviser or his client or any such representative and any other person, which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings. It does not include communications and items in the possession of a person who is not entitled to possession of them, and communications and items held, or oral communications made, with the intention of furthering a criminal purpose.
- Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.
- Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

## **2.13 General Observation**

2.13.1 General observation forms part of the duties of many law enforcement officers and other public authorities and Authorisations are not usually required. For example, officers might covertly observe and then visit a shop as part of their enforcement function. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

## **2.14 Use of the Council's CCTV system**

2.14.1 The use of Council's CCTV system is detailed in the CCTV manual located in the CCTV control room. This manual covers the use of the CCTV for surveillance purposes and must be followed at all times when conducting surveillance activities. Where CCTV is used overtly the guidance on the Implications for Public Space Surveillance in the light of the Data Protection Act 1998 produced by the Home Office must be followed, this can be found at <http://www.crimereduction.homeoffice.gov.uk/cctv/cctv7.htm>

## **2.15 Keeping Records**

2.15.1 All Investigating Officers have a legal obligation to keep accurate and full records of investigations under the Criminal Investigations and Procedures Act 1996 - Code of Practice. The Surveillance Code of

Practice puts an additional obligation on officers to maintain such records.

2.15.2 Records of the surveillance authorisations should be maintained by all staff involved in the process. The authorisations and current position should be summarised and maintained on the authorisation matrix (**Form RIPA 5**) and presented to the Authorising Officer at each review (**Form RIPA 4**).

2.15.3 Copies of the risk assessments, authorisations, renewals, reviews and cancellations given should be retained on the investigation file, the investigation file must be kept in a secure location. In particular, for the purposes of the Surveillance Code of Practice, Investigating Officers must keep in the investigation file:

- Reasons for any application for an oral application for authorisation;
- An account of events observed and/or conversations overheard;
- A full account of any surveillance which has taken place (undertaken in order to maintain contact with the moving target or to assess whether the target has been lost);
- Reasons for and the nature of collateral intrusion -and the results;
- Reasons for selecting a target when authorised only for general observations, without a specified target.

The Investigating Officer's official notebook is used to maintain the account of the events observed and heard.

2.15.4 The Director of Law and Democratic Services is responsible for monitoring and maintaining a central register of authorisations issued (**Form RIPA 5**). Copies of all authorisations, renewals, reviews and cancellations should be forwarded to the Director of Law and Democratic Services as soon as reasonably practicable after their completion.

## **2.16 Communications Data**

### **2.16.1 What is communications data?**

Communications data does not include the contents of a communication of any telephone or email communication but does include:

- Information about communications (traffic data);
- Information about the use of communications services (service use data);
- Information about communications service users (subscriber data).

Local Authorities currently do not have access to 'traffic data'. Any request for communications data must start with 'subscriber data'.

‘Service use’ data cannot be sought unless ‘subscriber data’ has already been obtained.

### 2.16.2 **Obtaining communications data**

Communications data can be obtained by way of a notice given to the communications data provider to collect or retrieve the data and provide it to the public authority, or through an authorisation that allows the public authority to collect or retrieve the data itself. In most cases the data should be sought by way of a notice.

### 2.16.3 **Applications**

Applications to obtain communications data must be sought through the Authority’s Single Point of Contact (SPOC) using **Form RIPA 6**. The SPOC may reject the application; otherwise the authorisation must be given to obtain the data by the Designated Person using **Form RIPA 6**. The Designated Persons and SPOC are listed in Appendix B.

### 2.16.4 **Renewal and Cancellations**

Authorisations and notices are valid for 1 month and they may be renewed at any time during that month. The Designated Person shall cancel a notice as soon as it is no longer necessary, or the conduct is no longer proportionate, by using **Form RIPA 8** and the communications data provider will be notified of any cancellation using **Form RIPA 9**.

### 2.16.5 **Disclosure and Retention of Data**

Disclosure will be made to the SPOC. Communications data and all copies, extracts and summaries of it must be handled and stored securely in compliance with the requirements of the Data Protection act 1998. The authority must retain applications, authorisations, and notices for communications data until they have been audited by the Commissioner. The authority should also keep a record of the dates on which the authorisation or notice started and was cancelled. Where any errors in the granting of authorisations or notices occur, a record should be kept and a report and explanation sent to the Commissioner.

### 2.16.6 **Data Retention**

The Data Retention (EC Directive) Regulations 2007 require public communications providers to retain certain data to enable public authorities to undertake their lawful activities to investigate detect and prosecute serious crime. The Regulations relate exclusively to traditional fixed line and mobile telephony. The contents of phone calls or text messaging can be required providing the investigating officer can demonstrate it is necessary and proportionate to do so. Officers should follow the procedures for acquiring communications data.

## **2.17 Encryption**

### **2.17.1 What is Encryption?**

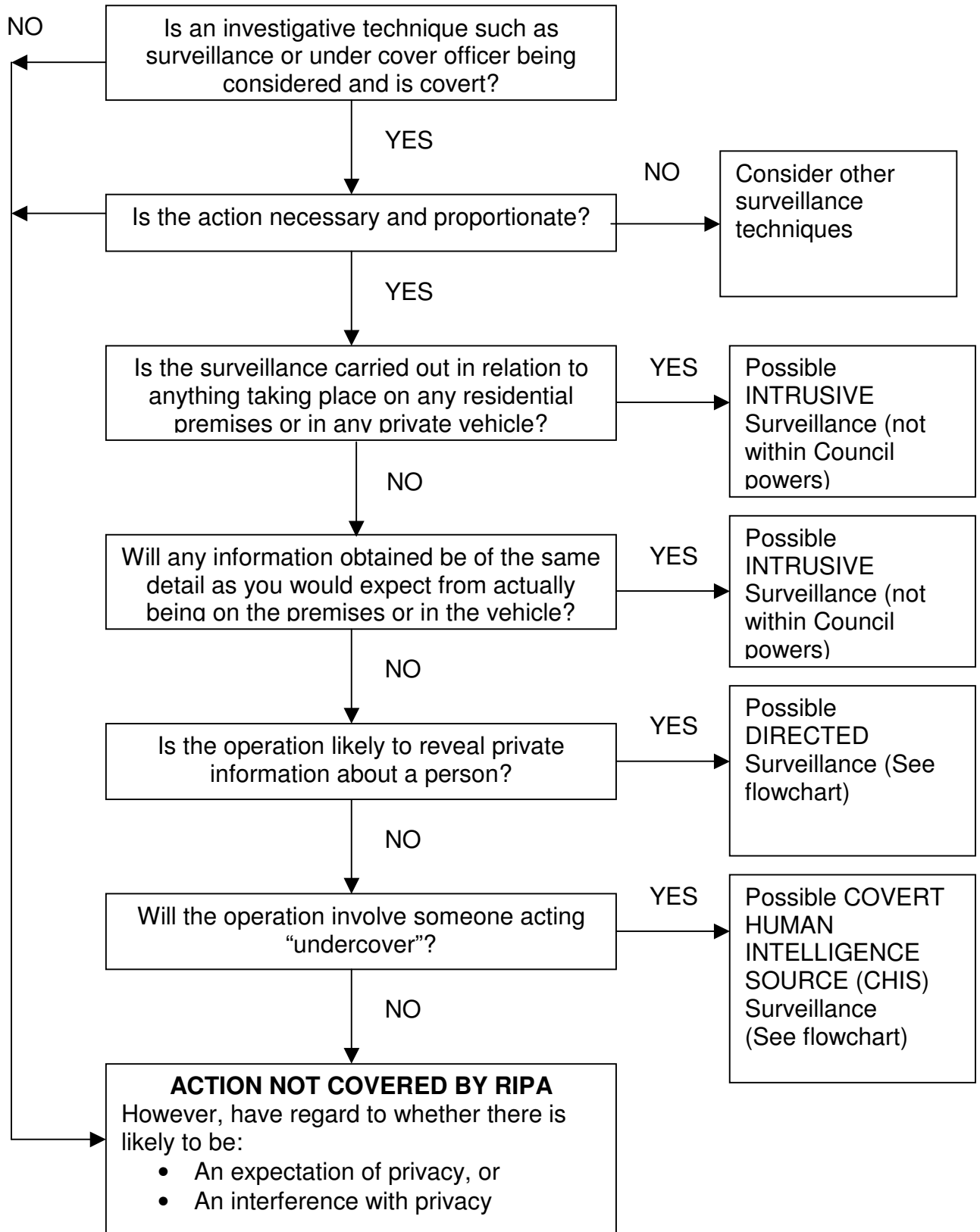
Encryption is the conversion of data into a form that renders the contents unintelligible to anyone not authorized to read it. Decryption is the process of converting the encrypted data back into its original form, so it can be understood. Many people use easily-accessible programmes to encrypt their email, files, folders, documents and pictures. However, these technologies are also used by terrorists, criminals and paedophiles to conceal their activities.

Part III of RIPA deals with the 'Investigation of Electronic Data Protected by Encryption etc'. It provides any public authority the power to require that data they have obtained or expect to obtain lawfully should be put into an intelligible form or to require disclosure of the means to make it intelligible.

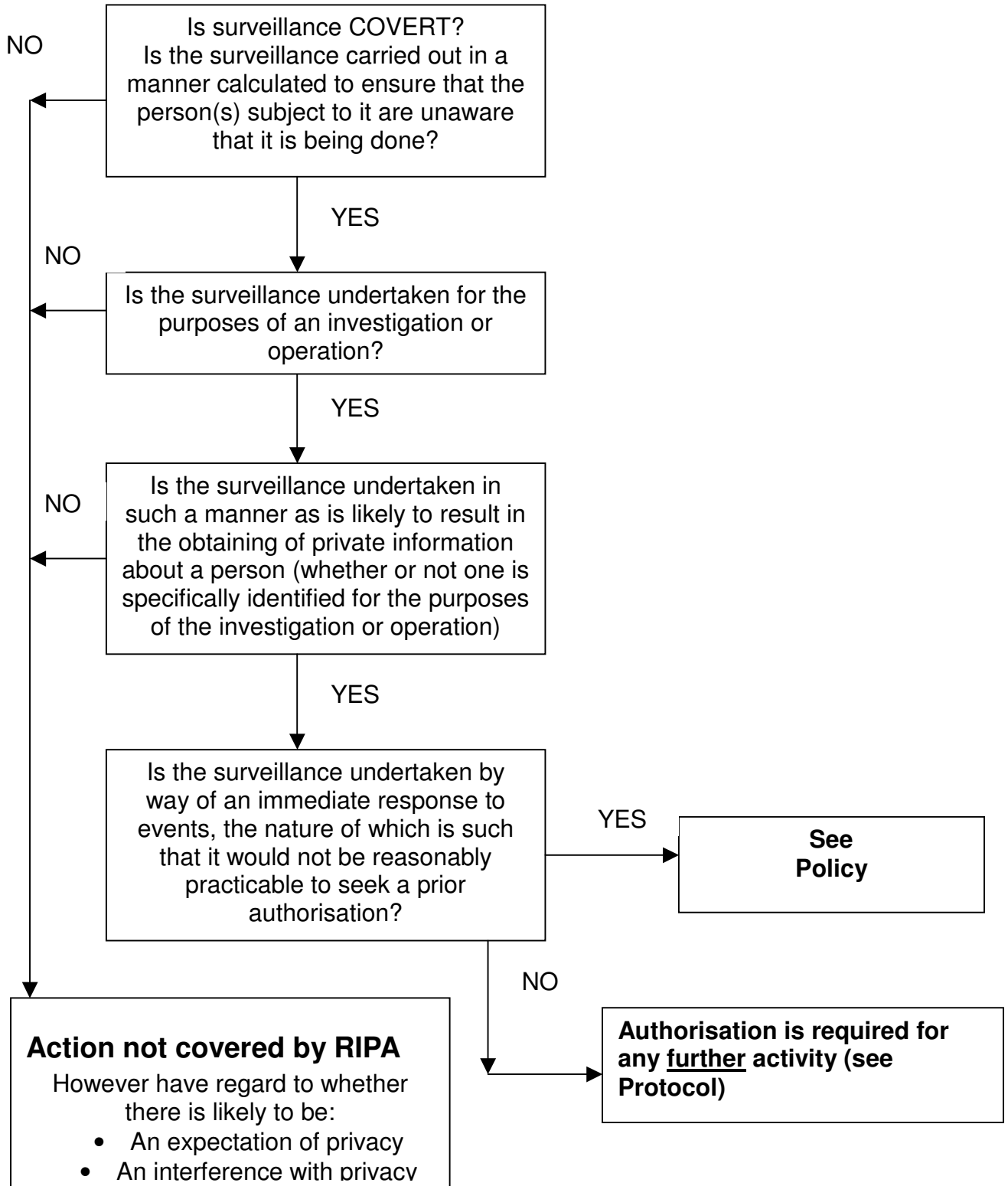
### **2.17.2 How to use encryption powers**

When using encryption powers refer to the 'Investigation of Protected Electronic Information: Code of Practice'.

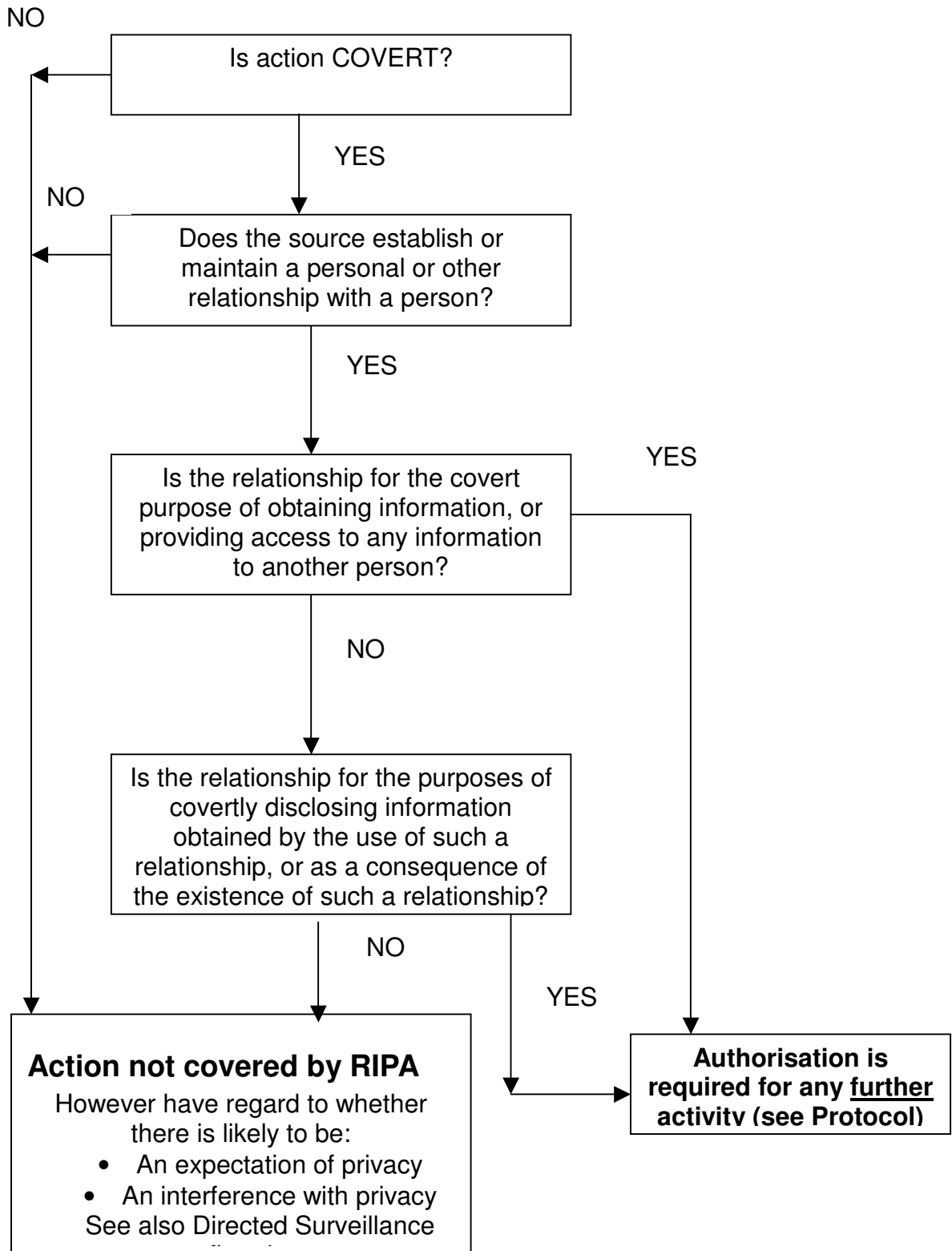
**TABLE 1 FLOW CHART – IS AUTHORISATION REQUIRED?**



## DIRECTED SURVEILLANCE



## COVERT HUMAN INTELLIGENCE SOURCES



## Appendix A – RIPA Forms

FORMS	TITLE	LINK
<b>RIPA 1</b>	Part II Application for Authorisation (Directed Surveillance).	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/application-directed-surveillanc?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/application-directed-surveillanc?view=Binary</a>
<b>RIPA 2</b>	Application for a Renewal of Authorisation for Surveillance	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/renewal-directed-surveillance?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/renewal-directed-surveillance?view=Binary</a>
<b>RIPA 3</b>	Cancellation of Authorisation (Directed Surveillance).	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/cancellation-directed-surveillan?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/cancellation-directed-surveillan?view=Binary</a>
<b>RIPA 4</b>	Review of Authorisation (Directed Surveillance).	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/review-directed-surveillance?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/review-directed-surveillance?view=Binary</a>
<b>RIPA 5</b>	Authorisation Matrix (Directed Surveillance)	
<b>RIPA 6</b>	Application for Communications Data	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/communications-data.doc?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/communications-data.doc?view=Binary</a>
<b>RIPA 7</b>	Notice Under Section 22(4) of the RIPA 2000 Receiving Communications Data to be Obtained and Disclosed	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/ripa-section-22-notice?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/ripa-section-22-notice?view=Binary</a>
<b>RIPA 8</b>	Cancellation of a Request for Communication Data.	
<b>RIPA 9</b>	Notice of Cancellation to be Sent to the Communication Provider.	
<b>RIPA10</b>	Part II Application for	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-application?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-application?view=Binary</a>

	Authorisation (CHIS).	
<b>RIPA11</b>	Review of A covert human intelligence source (CHIS) authorisation.	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-review?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-review?view=Binary</a>
<b>RIPA12</b>	Application for renewal of a covert human intelligence source (CHIS) authorisation	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-review?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-review?view=Binary</a>
<b>RIPA13</b>	Cancellation of an authorisation for the use or conduct of a covert human intelligence source	<a href="http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-cancellation?view=Binary">http://security.homeoffice.gov.uk/ripa/publication-search/ripa-forms/chis-cancellation?view=Binary</a>

## Appendix B – Authorising Officers

The Council has designated the following officers to authorise surveillance:-

<b>Designation</b>	<b>Officer</b>	<b>Scope</b>
Chief Executive	Gavin Jones	All purposes (including where there is a likelihood of acquiring confidential information)
Group Director of Environmental & Regeneration	Celia Carrington	All purposes (including where there is a likelihood of acquiring confidential information, but only in the absence of the Chief Executive)
Group Director of Business Transformation	Hitesh Patel	All purposes (including where there is a likelihood of acquiring confidential information, but only in the absence of the Chief Executive)
Group Director of Housing & Social Care	Caroline Fowles	All purposes (including where there is a likelihood of acquiring confidential information, but only in the absence of the Chief Executive)
Group Director of Children	John Gilbert	All purposes (including where there is a likelihood of acquiring confidential information, but only in the absence of the Chief Executive)
Director of Finance	Stuart McKellar	Fraud Investigation Purposes
Head of Internal Auditor	Nick Hobbs	Fraud Investigation Purposes
Fraud Manager	Michael O'Sullivan	Benefits

<b>Designation</b>	<b>Officer</b>	<b>Scope</b>
Director of Planning & Transportation	Dave Potter	Environmental Health Trading Standards Planning Trees Environmental Crime Taxis Anti Social Behaviour
Director (Children & Families)	Jean Pollard	Child protection
Director of Swindon Commercial Services	Bill Fisher	Fly Tipping CCTV
Director of Housing	Bernie Brannan	Housing
Resource Centre manager	Peter Holohan	Housing
Head of Regulatory Services	Phil Thomas	Trading Standards Environmental Health Environmental Crime Planning Trees Taxis Anti-Social Behaviour Single Point of Contact for Acquiring Communications Data
Head of Residential Services	Paul Simmonds	Environmental Health Trading Standards Environmental Crime Anti Social Behaviour
Policy & Regeneration Manager	Mark Walker	Housing

<b>Designation</b>	<b>Officer</b>	<b>Scope</b>
Trading Standards Manager (Bristol City Council)	Stephen Meale	Illegal Money Lending and scambuster operations

## **Appendix C - Codes of practice**

Covert Surveillance Code of Practice (01/11/2005)

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/covert-cop?view=Binary>

Covert Human Intelligence Code of Practice (26/09/2005)

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/human-cop?view=Binary>

Interception of Communications Code of Practice (24/11/2005)

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/interception-cop?view=Html>

Investigation of Protected Electronic Information Draft Code of Practice (29/06/2007)

<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/electronic-information?view=Binary>