

STAFFORD BOROUGH COUNCIL

SURVEILLANCE POLICY AND PROCEDURES



JANUARY 2009

CONTENTS PAGE

		Page No
A	Introduction and Key Messages	3
B	Background to the relevant Acts	4
C	What RIPA Does and Does Not Do	5
D	Types of Surveillance	6
E	Conduct and Use of a Covert Human Intelligence Source (CHIS)	9
F	Codes of Practise for Covert Surveillance / Use of a CHIS	11
G	Procedures for Conduct of / Authorisation Of Surveillance	12
H	Officers Permitted to Authorise a Covert Surveillance Exercise	16
I	Acquisition and Disclosure of Communications Data....	17

Annex 1 - Purpose of the RIPA and the Codes of Practice

Annex 2 – RIPA Flow Chart

A. Introduction and Key Messages

1. This Surveillance Policy is based upon the requirements of the Regulation of Investigatory Powers Act 2000 ('RIPA') and Home Office's Codes of Practices on Surveillance which support RIPA.
2. The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Head of Law & Administration for advice and assistance.
3. A copy of this document is on the Intranet and is reviewed annually.
4. The Head of Law & Administration is responsible for maintaining the central Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. The Head of Law & Administration is also responsible for :-
 - specifying, by name, appropriate officers able to grant RIPA authorisations (i.e. Authorised Officers)
 - verifying the competency of those officers before authorising them.
5. It is the responsibility of the relevant Authorised Officer, however, to ensure that the original forms are sent to the Head of Law & Administration. Authorised Officers must also ensure that, when sending the completed forms to the Head of Law & Administration they are conveyed in a confidential manner.
6. RIPA and this document are important for the effective and efficient operation of the Borough Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This document will, therefore, be kept under annual review by the Financial Services Manager.
7. In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the Council's e-mail and internet policies and guidance, and legislation such as RIPA, subsequent statutory instruments relating to RIPA the Data Protection Act 1998 Human Rights Act 1988 etc. RIPA forms should be used where **relevant** and they will be only **relevant** where the **criteria** listed on the Forms are fully met.
8. Covert Surveillance may be used by Stafford Borough Council for the investigation of employees.

B	Background to the Relevant Acts
----------	--

- 1 Under legislation it is the responsibility of all public bodies to comply fully with the requirements of the Human Rights Act (HRA) 1998 which came into force on the 2nd October, 2000. The Regulation of Investigatory Powers Act (RIPA) 2000 was enacted in order to give a clear statutory framework for the operation of certain intrusive investigative techniques, to provide for compliance with the HRA. RIPA also provided for the appointment of independent Surveillance Commissioners to oversee the exercise by public authorities of their powers and duties under the act.

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

- 3 Essentially RIPA requires the following human rights principles to be complied with for investigatory work:-
 - the proposed action must be lawful
 - the proposed action must be proportionate
 - the proposed action must be necessary
 - the proposed action must be non-discriminatory.

- 4 To coincide with the RIPA coming into force, the Home Office published four statutory Codes of Practise, which are mandatory under the terms of the Act (Part IV, para 75(1), covering:-
 - * Use of covert surveillance
 - * Use of covert human intelligence sources
 - * Interception of communications and accessing communications data
 - * Investigation of electronic data protected by encryption.

Details of the Codes are attached as ANNEX 1 to this Policy & Procedures Document.

- 5 The Regulation of Investigatory Powers Act states that all public authorities (including local authorities) are expected to comply with the Codes.

- 6 The codes of practise which have the most significant impact on the activities of officers at Stafford Borough Council (SBC), are the Code of Practise on Covert Surveillance and the Code of Practise on the Use of Covert Human Intelligence Sources (CHIS). However, officers should also be aware of the Regulation of Investigatory Powers (Communications Data) Order which provides guidance on the acquisition and disclosure of communications data. For any covert surveillance (and acquisition / disclosure of communications data) to be lawful, RIPA must be complied with.

C What RIPA Does and Does Not Do

1. RIPA does:

- require prior authorisation of directed surveillance.
- prohibit the Council from carrying out intrusive surveillance.
- require authorisation of the conduct and use of a CHIS.
- require safeguards for the conduct and use of a CHIS.

2. RIPA does not:

- make unlawful conduct which is otherwise lawful.
- prejudice or dis-apply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

3. If the Authorised Officer or any Applicant is in any doubt, he / she should ask the Head of Law and Administration BEFORE any directed surveillance and / or CHIS is authorised, renewed, cancelled or rejected.

4. A **Single Point of Contact (SPOC)** is required under the RIPA (Communications Data) Order 2003. All Local Authorities have at least one accredited SPOC. The officers undertaking this role within Stafford Borough Council are referred to below. The SPOC is to enable and maintain effective co-operation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data.

D. Types of Surveillance

1. **Surveillance** is defined as including:-

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

2. There are different types of surveillance:-

- general surveillance (not directed at an individual)
- covert surveillance (directed / intrusive).

RIPA authorisation is not required for all surveillance. It only applies to covert surveillance:

3 **Overt Surveillance**

3.1 Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and / or will be going about Council business openly (e.g. a community warden on patrol).

3.2 Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner / proprietor to check that the conditions are being met.

4. **Covert Surveillance**

4.1 In terms of RIPA an action is defined as **covert** “if, and only if, it is carried out in a manner that is calculated to ensure that the persons who are subject to surveillance are unaware that it is or may be taking place”

4.2 RIPA regulates two types of covert surveillance, Directed Surveillance and Intrusive Surveillance and the use of Covert Human Intelligence Sources (CHIS).

5. **Directed Surveillance**

5.1 Surveillance is directed if it is undertaken:

- for the purpose of a specific investigation or specific operation in such a manner as is likely to result in the obtaining of private information about a

person (whether or not that person is specifically targeted for purposes of an investigation), and

- is covert , and
- is not intrusive surveillance (see definition below – the Council must not carry out any intrusive surveillance), and
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it

5.2 The key issue in Directed Surveillance is the targeting of an individual with the intention of gaining private information. This includes any information relating to private and family life, home and correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

5.3 Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

6. Intrusive Surveillance

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

6.2 Surveillance is intrusive if it:-

- is covert
- is carried out in relation to anything taking place on any residential premises or in any private vehicle
- involves the presence of an individual in the premises or in the vehicle or is carried out by a surveillance device in the premises / vehicle. cameras, tape recorders etc.

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

Intrusive Surveillance can be carried out only by the police and other law enforcement agencies. Council officers must not carry out intrusive surveillance.

7. Examples of different types of Surveillance

Type of Surveillance	Examples
<u>Overt</u> does not require RIPA Authorisation	<ul style="list-style-type: none"> - Police Officer or Parks Ranger on patrol - Signposted Town Centre CCTV cameras (in normal use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Sampling purchases (where the officer behaves no differently from a normal member of the public). - Dog Warden in uniform on patrol in park, street or van - Food Safety or Health & Safety Inspections
<u>Covert</u> but not requiring prior authorisation	<ul style="list-style-type: none"> - CCTV cameras providing general traffic, crime or public safety information.
<u>Covert Directed</u> must be RIPA authorised.	<ul style="list-style-type: none"> - Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or has long term sick leave from employment. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner. - Surveillance of a property in relation to the movement or selling of illegal food products - Fly tipping surveillance
Intrusive – Council cannot do this!	<ul style="list-style-type: none"> - Planting a listening or other device in a person's home or in their private vehicle.

E. Conduct and Use of a Covert Human Intelligence Source (CHIS)

1. A person is a covert human intelligence source (CHIS) if he / she establishes or maintains a personal or other relationship with a person for the covert purpose of using the relationship to obtain information.
2. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information.
3. If information is received via Hotline or similar, this does not constitute a CHIS. Guidance is not to ask the informant to gather information on our behalf, as this may result in forming a relationship with the subject and therefore becoming a CHIS.
4. It is most unlikely that it will ever be appropriate for the Council to utilise a CHIS. In the event that it is ever considered, advice should be sought from the Head of Law & Administration at an early stage.
5. **What must be authorised?**
 - 5.1.1 The Conduct or Use of a CHIS requires prior authorisation.
 - **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
 - **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.
 - 5.1.2 **The Council can use CHIS's IF, AND ONLY IF, RIPA procedures, detailed in this document are followed**
6. **Juvenile Sources**
 - 6.1 Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents. The Head of Law & Administration must be contacted re the potential use of Juvenile Sources as there are other onerous requirements for such matters.
7. **Vulnerable Individuals**
 - 7.1 A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

7.2 A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. The Head of Law & Administration must be contacted re the potential use of Vulnerable Individuals as there are other onerous requirements for such matters.

8. Test Purchases

8.1 Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

8.2 By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products will require authorisation as a CHIS). Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

9. Anti-social behaviour activities (e.g. noise, violence, race etc)

9.1 Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

9.2 Recording sound (with a Digital Audio Type recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

F Codes of Practise For the Use of Covert Surveillance / Use of a CHIS

1. The use of directed surveillance or covert human intelligence sources (CHIS) for a particular investigation must be subject to prior authorisation by an officer of a rank or position at least as senior as is specified in Regulations made under RIPA. For local authorities this is “Assistant Chief Officer” or “officer responsible for the management of an investigation”.
2. The use of directed surveillance or covert human intelligence sources should only be authorised if the authorising officer is satisfied that:-
 - (a) the action is necessary (in a democratic society) for the prevention or detection of crime or the prevention of disorder
 - (b) the surveillance is proportionate - the HRA defines a measure or action as proportionate if it:
 - * impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties)
 - * is carefully designed to meet the objectives in question
 - * is not arbitrary, unfair or based on irrational considerations.
3. Essentially the person granting the authorisation must believe that the use of a source is proportionate to what is sought to be achieved by the conduct and use of that source. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.
4. Any surveillance involved in a case, even if it does not form part of an eventual prosecution case, will be deemed unlawful if not properly authorised and could lead to a challenge under Article 8 of the ECHR.
5. The requirements of the RIPA and the HRA impact on all officers of the Council who undertake investigatory or enforcement activities, including Benefits Fraud Investigation, Health, Planning and Internal Audit. **The Council adopts the Codes of Practice which are mandatory under the Act, and the following procedures should be adhered to in the conduct of any covert surveillance.**

<p>G. Procedures for Conduct of / Authorisation of Surveillance (See Annex 2 for Flow Chart)</p>

- 1 Staffordshire Police have simplified RIPA by the acronym - "PLAN" ie covert surveillance must be proportional, lawful, authorised and necessary:-
 - * proportional (not using a sledgehammer to crack a nut)
 - * lawful (in accordance with legislation and the legality of the audit activity)
 - * authorised (by a proper person)
 - * necessary (having considered alternatives).

- 2 For any covert surveillance to be lawful, records must be sufficient to prove that RIPA has been complied with. All procedures relating to covert surveillance must be documented on standard forms. These are referred to below. The latest versions of the documents can be downloaded from the Government website on the internet www.homeoffice.gov.uk

- 3 Covert surveillance carried out by an officer of the Council should be subject to prior authorisation by a "senior" officer within the Council. It should not be authorised by an officer directly involved in the surveillance so that there is independent review of whether the surveillance is necessary and proportionate. Officers designated to authorise surveillance are detailed in section H below.

- 4 Application for authorisation should be made in writing except in urgent cases and these should include full details of the proposed surveillance and the duration. **See attached for copies of the Application forms.** The application must include full details of:
 - the grounds on which the action is necessary
 - why the action is proportionate to what it seeks to achieve (there must be a clear indication of what alternative methods were considered for obtaining the information required and why these were rejected) It may be useful to state that this is the only way the evidence can be gathered.
 - the person(s) to be subject to the action
 - the action to be authorised (ie observation / following and reference to any premises/vehicles involved and whether private / public, residential/business)
 - full description of the work to be carried out (including locations of areas from which observations are to be conducted eg street names etc and whether photography equipment or binoculars are to be used)
 - an account of the investigation / operation
 - the information which is sought from the action
 - the potential for collateral intrusion and a plan to minimise this potential (ie the potential impact on other people not involved in the action)
 - the likelihood of acquiring any confidential/religious material (medical records, financial records, legal documents etc).

- 5 A higher level of authorisation is required in respect of confidential / religious material. In all such cases authorisation should be obtained from the Chief Executive.
- 6 Where surveillance is reactive (ie an immediate response to an immediate situation) this must be documented within reasonable time of the surveillance. Staffordshire police have indicated the time limit as being 3 days.
- 7 The authorising officer must consider whether the proposed surveillance is proportionate, lawful, necessary and non discriminatory. The criteria for surveillance is listed on the application forms. If the proposed surveillance cannot be embraced within the criteria it should not be undertaken.
- 8 Surveillance activity must be proportionate to the offence under investigation. For example suspected theft from the workplace may merit surveillance at work but not at the person's home. The length of the investigation also needs to be proportionate.
- 9 In assessing whether or not the proposed surveillance is proportionate, consideration should be given to other appropriate means of gathering the information. **The least intrusive method will be considered proportionate by the courts.**
- 10 Account must be taken of the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise collateral intrusion and the matter may be an aspect of determining proportionality.
- 11 The appropriate course of action must then be decided in terms of the type of surveillance and hence the appropriate form / course of activity:-
 - directed surveillance
 - intrusive surveillance – not to be undertaken by local authority
 - use of a Covert Human Intelligence Source.
- 12 Intrusive surveillance is only allowed for “serious” crimes. The police can only obtain authorisation for intrusive surveillance from the Surveillance Commissioners. Local authorities cannot undertake intrusive surveillance.
- 13 There must be appropriate arrangements in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment.
- 14 Any surveillance should have a dedicated log-sheet for officers use (**see attached for copy of sheet currently utilised by Internal Audit & Benefits Fraud Investigation**). The log-sheet should be kept in chronological order detailing who is on the surveillance, where it is and what happens. Where notes cannot be written up at the time of surveillance it should be completed as soon as possible afterwards.

- 15 All alterations in the log sheet should be crossed through and initialled and then the corrected material written to the side in the normal manner. Correction fluid should not be used at any time. Completion of the log should ensure that no empty lines are left where additional information could be written in at a later date. These logs could be used in the event of criminal prosecution and should be kept correctly, signed as true statements, and secure at all times.
- 16 In all cases there is a duty of care to those surveyed. All details and approvals must be kept strictly confidential. The privacy of individuals must not be put at risk and unnecessary information should not be documented i.e. if the observed person was incidentally observed in a private context such as an extra marital affair.
- 17 Where photographs or videos are taken then a photographic log needs to be maintained and all negatives retained. Technology is available to alter photographs and the logs are important to prove the originality of the photographs / videos.
- 18 Log sheets should be kept locked with the rest of the supporting documents for a period of 6 years.
- 19 All authorisations should be held at a central point to facilitate independent examination by the Surveillance Commissioners. Copies of all authorisations and cancellations should therefore be forwarded to the Head of Law & Administration.
- 20 A review date should be set for the authorisation and be reviewed no later than that date.
- 21 With regard to the duration of an authorisation, cancellation must be a positive act for which diary dates are set. Time limits should be placed on any authorisation for surveillance. In all cases written "Authorities" last for 3 months and then must be renewed if that is deemed necessary provided they meet the requirement for authorisation. Authorisation should be cancelled as soon as they are considered to be no longer necessary or appropriate. Forms are available for the cancellation and the renewal of surveillance as required.
- 22 **Urgent Authorisations** should not be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. It will not be urgent where the need for authorisation has been neglected or is of the Officer's own making.

Urgent authorisations last for no more than 72 hours. They must be recorded in writing on the standard form as soon as practicable and the extra boxes on the form completed to explain why the authorisation was urgent.

H. Officers Permitted to Authorise a Covert Surveillance Exercise
--

1. The Surveillance Policy and Procedures as set out in this document will become operative with effect January 2009. It is essential, therefore, that the Leadership Team and other Authorised Officers take personal responsibility for the effective and efficient operation of this document.
2. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.
3. The Head of Law & Administration will ensure that sufficient numbers of Authorised Officers from each Service are, after suitable training on RIPA and this document, duly certified to take action under this document.
4. It will be the responsibility of Authorised Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'Applicants' so as to avoid common mistakes appearing on Forms for RIPA authorisations.
5. Authorised Officers will also ensure that staff who report to them follow this Surveillance Policy & Procedures document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.
6. Authorised Officers must also pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorised Officer approve any RIPA form unless, and until s/he is satisfied the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If an Authorised Officer is in any doubt, s/he should obtain prior guidance on the same from the Head of Law and Administration.
7. The officers permitted to authorise a covert surveillance exercise at Stafford Borough Council (i.e. the Authorised Officers) are:-
 - (a) **Internal Audit - Financial Services Manager / Head of Finance ; the latter if the former is involved in the surveillance.**
 - (b) **Benefits Fraud Investigation - Revenues & Benefits Manager / Head of Finance ; the latter if the former is involved in the surveillance.**
 - (c) **Other departments – the relevant Head of Service .**
8. Prior to operating their powers to authorise surveillance, such officers must have undertaken such training as deemed appropriate by the Head of Law & Administration, A record of officers who have undertaken training will be kept by the Head of Law & Administration.

I. Acquisition & Disclosure of Communications Data

- 1 Communications data is information held by communication service providers (e.g. telecom, internet and postal companies). The Act makes provision for obtaining communications data from such service providers and the disclosure to any person of such data. 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.
- 2 Examples of “data” available to the Council under the Act include:-
 - postal item (anything written on the outside of the envelope)
 - telephone (personal details of the subscriber, the telephone number and itemised calls made)
 - e-mail and internet (details of the subscriber of email account, websites visited, details of the date and times emails sent and received).
- 3 Similarly the procedures relating to both directed surveillance and CHIS, communications data can only be obtained for the sole purpose of the prevention / detection of crime and / or disorder. Further the test of **necessity** must be met before data is obtained. The assessment of necessity is made by an authorising officer as set out in 3.3 above. The authorising officer must also consider the conduct involved in obtaining the communications data to be **proportionate** to what it is sought to achieve, and must also consider the risk of collateral intrusion.
- 4 Communications data can be accessed using 2 different methods :-
 - the granting of Authorisations, or
 - the service of Notices.
- 5 An authorisation would allow the Council to collect or retrieve the data itself from the service provider. A notice is given by the Council to a postal or telecommunications operator and requires that operator to collect the data and provide it to the Council.
- 6 Integral to the acquisition of communications data under RIPA is the Single Point of Contact (SPoC). The role of the SPoC is to enable and maintain effective co-operation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data.
- 7 SpoCs must be properly trained in accordance with Home Office guidelines and must register their details with the Home Office.
- 8 The Officer currently designated as the Council’s Single Point of Contact for enquiries is the Legal Services Manager. Further officers are to be trained in this role and the details of those accredited as SPOCs will be kept on a list maintained by the Head of Law & Administration.

CABINET - 27 JANUARY 2009 - RESOURCES

Purpose of the RIPA and the Codes of Practice**Purpose of the Act**

The purpose of the Act is to regulate *“the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or access.”*

The Codes of Practice

The Home Office has published four statutory Codes of Practice, which are mandatory under the terms of the Act (Part IV, para 75(1)). The title of each Code, along with a brief description of the purpose of each Code (Taken from the Codes themselves) is given below:-

Code of Practice on the Use of Covert Surveillance

Surveillance plays a necessary part in modern life. It is used not just in the targeting of criminals but as a means of protecting the public from harm and preventing crime.

The covert surveillance covered by this code is in two categories: intrusive surveillance and directed surveillance. The code defines the two categories and the authorisation procedures for both. Authorisation for covert surveillance gives lawful authority to carry out surveillance. However, often surveillance operations will also involve interference with property. This requires separate authorisation and Part 5 of this code details the procedures which give lawful authority for the interference with property and wireless telegraphy.

Neither do the provisions of the 2000 Act or of this code of practice cover authorisation for the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime.

Code of Practice on the Use of Covert Human Intelligence Sources

This code of practice provides guidance on the use and conduct of covert human intelligence sources by public authorities listed in Schedule 1 of the RIPA Act 2000.

A covert human intelligence source (“a source”) is defined in section 25(7) of the 2000 Act as a person who establishes or maintains a personal or other relationship with other person for the covert purpose of facilitating anything that:

- (a) covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- (b) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship

A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

Code of Practice on the Interception of Communications and Assessing Communications Data

This code of practice provides guidance on the use of interception of communications and accessing communications data authorised under Part 1 of the RIP Act 2000. It covers operations conducted by all the public authorities listed in these parts of the 2000 Act.

The RIPA (Communications Data) order specifies which individuals in public authorities are entitled to acquire communications data. It also places restrictions on the grounds on which they may acquire communications data and the types of communications data they may acquire.

Code of Practice on the Investigation of Electronic Data Protected by Encryption

Part III of the RIP Act 2000 establishes a power to require any person served with an appropriate notice to disclose protected (eg encrypted) information in an intelligible form (“plain text”). The Part III power is ancillary to all-statutory and non-statutory powers and functions of public authorities. Its use by any public authority requires proper and specific permission. A number of statutory requirements must be met before any such permission can be given to exercise the disclosure power. There are extra requirements where a decryption key - rather than plain text - is desired. The 2000 Act sets out statutory safeguards for the protection of all information obtained under the Part III power. There are associated offences. The Act also provides for independent oversight of the measures in Part III and an independent complains mechanism.

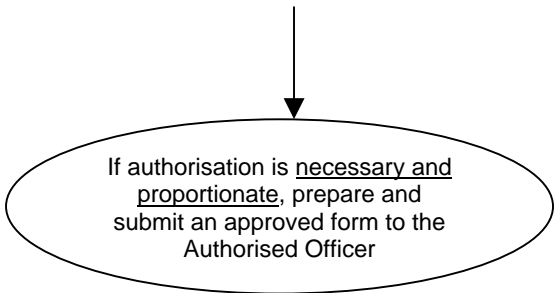
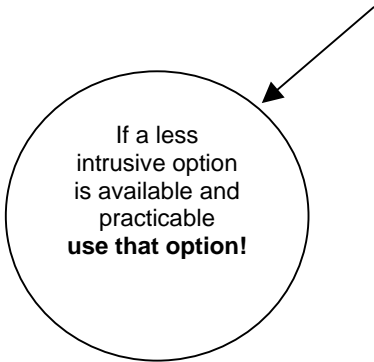
The Home Secretary has powers under the Act to issue new or revised Codes of Practice as he/she sees fit and all such Codes will be mandatory on all public bodies.

RIPA FLOW CHART

ANNEX 2

Requesting Officer ('The Applicant') must:

- Read the Surveillance Policy & Procedures document and be aware of any other guidance issued by the Head of Law & Administration.
- Determine that directed surveillance and/or a CHIS is required.
- Assess whether authorisation will be **in accordance with the law**.
- Assess whether authorisation is **necessary** under RIPA and whether it could be done overtly.
- Consider whether surveillance will be **proportionate**.
- Obtain RIPA form.
- If authorisation is approved – review regularly



- Authorised Officer must:**
- Consider in detail whether all options have been duly considered, including the Surveillance Policy & Procedures document and any other guidance issued by the Head of Law & Administration.
 - Consider whether surveillance is considered by him/her to be necessary and proportionate.
 - Authorise only if an overt or less intrusive option is not practicable.
 - Set an appropriate review date (can be up to 3 months after authorisation date) and conduct the review.

The Applicant must: REVIEW REGULARLY
Complete Review form and submit to Authorised Officer on date set.

The Applicant must:
If operation is no longer necessary or proportionate, complete **CANCELLATION FORM** and submit to Authorised Officer

- Authorised Officer must:** If surveillance is still necessary and proportionate:
- Review authorisation
 - Set an appropriate further review date

Authorised Officer must:
Cancel authorisation when it is no longer necessary or proportionate to need the same.

