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 EHCR. 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.

1.2.3 Local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences. These offenses must be either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco. They can only do so where prior approval from a JP has

been granted. These requirements do not apply to communications data or to the use of human intelligence resources. But the authorisation of a magistrate is needed for the use of all three forms of surveillance.

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
- Specimen directed surveillance application form.

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 25th September 2002 and has been subsequently revised. **This revision was issued in March 2016.**

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.

Proportionality 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. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity 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. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair".

This requires the officer to justify the need for the surveillance and the methods used and balance those with the impact on the privacy of the subject. The DCA guide on Human Rights (page 55) states:

"When taking decisions that may affect any of the qualified rights, a public authority must interfere with the right as little as possible only going as far as is necessary to achieve the desired aim."

To demonstrate proportionality, the following issues must be addressed here

Is this proposed use proportionate?

- ***To the seriousness of the offence or the mischief***
- ***To the degree of intrusion on the target and other people***
- ***Have other overt means been considered and discounted***

Factors to set out include:

- *Amount of information to be gathered during the surveillance*
- *Impact of surveillance on the subject*
- *Timing of the surveillance*

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, business, professional 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.

It is important to remember a relationship can be formed from a single encounter.

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. A CHIS Authorisation should be used. However if the premise is being used as a residential dwelling then the surveillance is consider to be intrusive surveillance and cannot take place.

(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.

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.

2.4.5 The 'Handler' will record information of the identity of the source on a log and will destroy all records which identify the 'CHIS' once the investigation has been completed.

2.4.6 The authority shall also appoint a 'Controller' who will have general oversight of the use made of the source.

2.4.7 Before a CHIS is used a risk assessment must be completed and kept with the application **Form RIPA 7.** This risk assessment should be reviewed at least monthly.

2.4.8 The use of a juvenile as a CHIS should generally be avoided and must only be used in exceptional circumstances. The Chief Executive is the only officer who can authorise an application to use a juvenile as a CHIS.

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.**

2.5.2 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.

2.6 Collateral Intrusion

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.

People who may be the subject of collateral intrusion include:

- Customers or workers at a business premises
- Visitors to a property
- Friends or relatives of the suspect

Firstly, identify here who else may be caught by the surveillance.

Secondly, state why it is unavoidable. This could be because of the nature of the premises (e.g. restaurant) or because of what the person is doing (e.g. visiting other subject/target premises) that there will always be third parties around who will be captured on film or whose activities will be recorded/observed in some way.

Thirdly set out what steps you have taken to minimise collateral intrusion. This may include:

- Using a still camera as opposed to a video camera
- If installing hidden cameras, only switching them on at specific times rather than all the time
- Narrowing the field of vision or the place where the cameras are cited
- Reducing the amount of surveillance done at busy times e.g. shops or places of worship

If you cannot minimise collateral intrusion you still need to show you have considered it. You may wish to add that you cannot do anything to minimise it but you will not be making any decisions on the information gathered about third parties unless it shows them committing a criminal offence.

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 RIPA7.**

- Obtain authorisation from an Authorised Officer. Appendix B lists the officer's the Council has designed as being able to authorise surveillance.

***Note**: As from March 2015 both the Authorising Officer and the Designated Person must be 'Operationally Independent' from any investigation they are considering or are involved with. . More information on this requirement is provided in Appendix B, along with details as to how the council will ensure that this requirement is met.*

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.

2.7.3 A specimen directed surveillance application form is set in **Appendix D.**

2.7.4 Before making an application for surveillance the investigating officer shall contact the PA to the Director of Law and Democratic Services to obtain an URN.

2.8 Time Limit on Written Authorisation

2.8.1 Written authorisation is valid for three months (unless cancelled), 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 8.** The Authorising Officer, after carrying out a review, should complete **Form RIPA 4** or CHIS **Form RIPA 9.**

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 7.** 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 10**) 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 Justice of the Peace Approval

2.11.1 No covert surveillance can be authorised without approval by a justice of the Peace. The process for obtaining approval is set out in table 2.

2.11.2 The applicant completes the application form and obtains authorisation in the usual way.

2.11.3 The applicant will provide the justice of the Peace (JP) with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration.

2.11.4 The original RIPA authorisation or notice should be shown to the JP but will be retained by the local authority.

2.11.5 In addition, the applicant has to provide the JP with a partially completed judicial application/order form (at Annex B).

2.11.6 The order section of this form will be completed by the JP and will be the official record of the JP's decision.

2.11.7 The applicant will need to obtain judicial approval for all initial RIPA authorisations/applications **and renewals** and the local authority will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

2.12 When Authorisation of Surveillance In or Into a Public Place is Not Required

2.12.1 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.

2.12.2 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 where private information is acquired, 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.sia.homeoffice.gov.uk/pages/licensing-cctv.aspx

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

2.15.3 Copies of the risk assessments, authorisations, JP Approval, 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. Originals of all authorisations, JP Approvals, renewals, reviews and cancellations should be forwarded to the Director of Law and Democratic Services as soon as reasonably practicable after their completion.

2.15.5 When an officer wishes to make an application to conduct any surveillance, they must contact the PA to the Director of Law and Democratic Services, who will provide a URN for the surveillance and will keep a central record of all application and authorisations. Officers must ensure that they update the PA to the Director of Law and Democratic Services, when the review, renew or cancel an authorisation and send at copy for the relevant paperwork to the PA to the Director of Law and Democratic Services,

2.16 RIPA Roles and Responsibilities

2.16.1 **Senior Responsible Officer** – is responsible for having daily over sight of the RIPA process by ensuring

- The integrity of the process in place within the public authority to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
- Compliance with Part II of the 2000 Act, Part III of the 1997 Act and with the codes;
- Engagement with the Commissioners and inspectors when they conduct their inspections,

- That all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of Surveillance Commissioners. Where an inspection report highlights concerns about the standards of authorising officers, this individual will be responsible for ensuring the concerns are addressed
- To review the quality of the applications and authorisations
- To authorize surveillance activities but only in exceptional circumstances.

2.16.2 **Coordinating Officer** – is responsible for ensuring all authorising officers and investigating officers are properly trained and to raise awareness of RIPA within the Authority.

2.16.3 **CHIS handler** – is responsible for the safety and security of the CHIS and the identity. The handler is also responsible for directing the day to day activities of the source and recording the information supplied by the source. 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.

2.16.4 **CHIS Controller** - be responsible for the general oversight of the use of the source.

2.16.5 **Authorising Officer** is responsible for ensuring that the application for surveillance is permitted to be undertaken by the local authority, to ensure that the proposed surveillance is necessary and proportionate and the any collateral intrusion is limited as far is practical. The authorising officer is responsible for determining the surveillance that can take place.

Note: *The Authorising Officer <u>must be independent</u> from any operation / investigation they are asked to consider. If this requirement cannot be shown to have been met OR if there is any uncertainty, then a different Authorising Officer who is independent must consider the application.*

2.16.6 **Elected members** - elected members of a local authority will review the authority's use of the 2000 Act and set the policy at least once a year. They will also consider internal reports on use of the 2000 Act on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

2.16.7 **Coordinating Officers Group** is responsible for ensuring that the procedures are being applied across the Authority. To ensure consistency of approach and application of RIPA.

2.16.8 PA to the Director of Law and Democratic Services is responsible

- For keeping the central register of RIPA authorisation
- Providing a URN for each RIPA application and
- Maintaining the records of applications, authorisations, reviews, renewals and cancellations.

2.17 Completion of Risk Assessments

2.17.1 When any directed surveillance or use of a CHIS is considered the applicant should produce a detailed risk assessment for the surveillance requested.

2.18 Communications Data

2.18.1 **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.

Whilst other forms of surveillance must be treated as a last resort, obtaining Communications Data should be the first resort in helping to identify offenders and victims.

2.18.2 **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.

2.18.3 **Applications**

Applications to obtain communications data must be sought through the Authority's Single Point of Contact (SPOC) using **Form RIPA 5**. The SPOC may reject the application; otherwise the authorisation must be given to obtain the data by the Designated Person using **Form**

RIPA 5. The Designated Persons and SPOC are listed in Appendix B. In the case of Service Data then **Form RIPA 11** must be completed by the investigating officer. NAFN guidance for obtaining magistrates authorisation must be followed. This guidance is set out in Appendix F.

2.18.4 **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, and the communications data provider will be notified of any cancellation.

2.18.5 **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.

2.18.6 **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.

2.19 Encryption

2.19.1 **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.

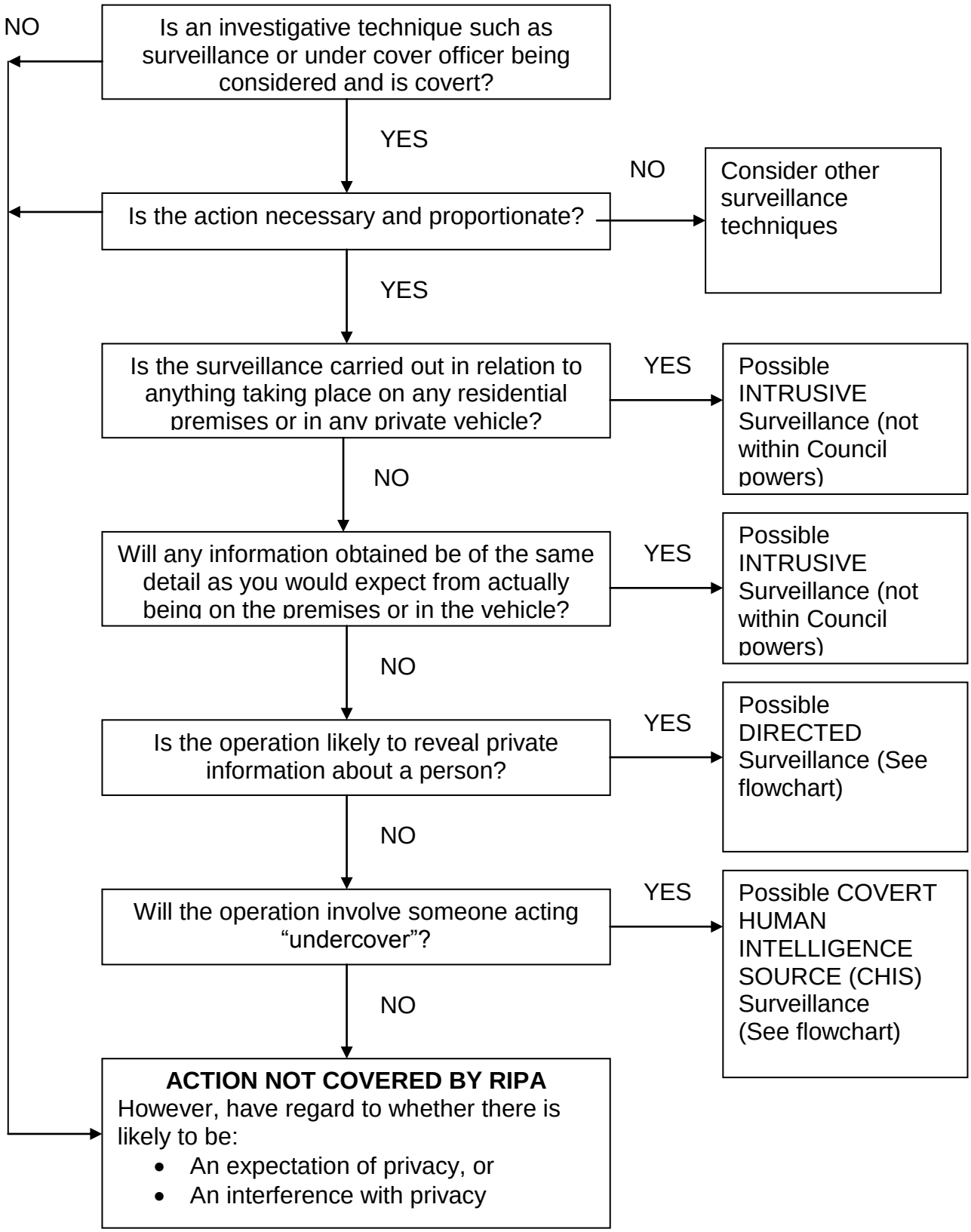
2.19.2 **How to use encryption powers**

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

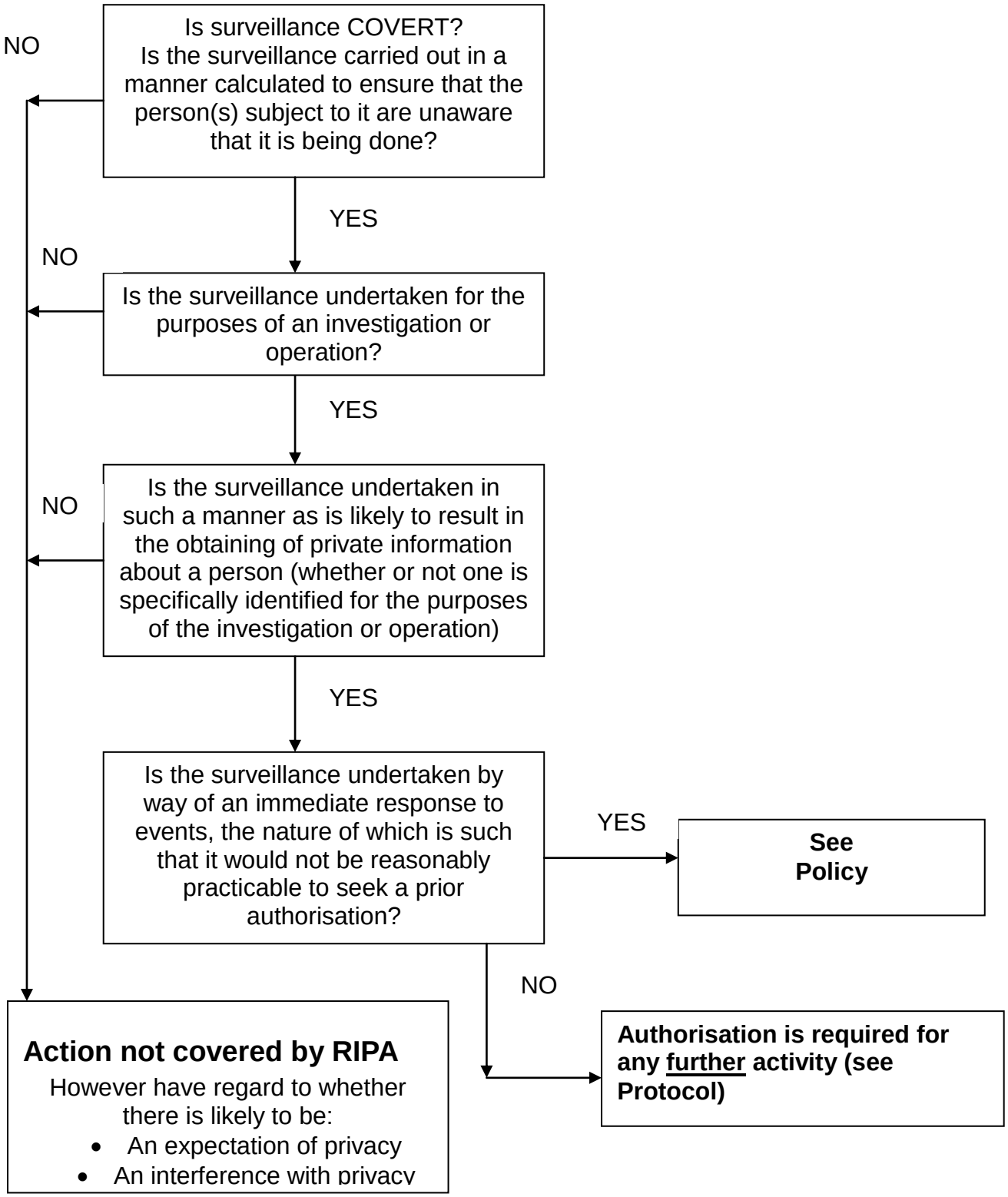
2.20 Training

2.20.1 No officer shall undertake any surveillance activity unless they have received training for RIPA. Every applying officer should undertake refresher training on every two years. Authorising officers should be regularly trained and if they do not authorise surveillance activities on a regular basis they should refresh their knowledge of RIPA before they authorise a request.

TABLE 1 FLOW CHART – IS AUTHORISATION REQUIRED?



DIRECTED SURVEILLANCE



COVERT HUMAN INTELLIGENCE SOURCES

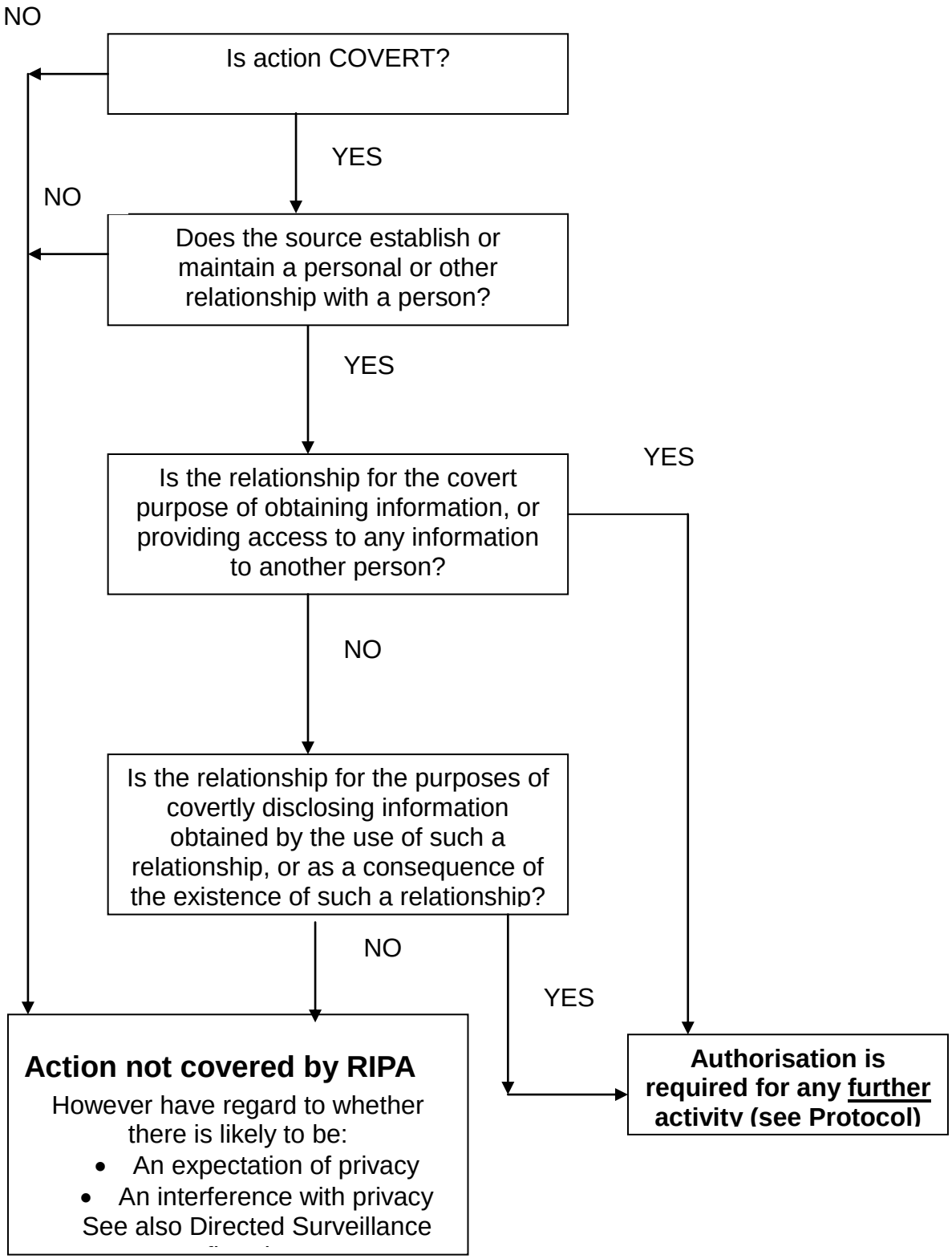
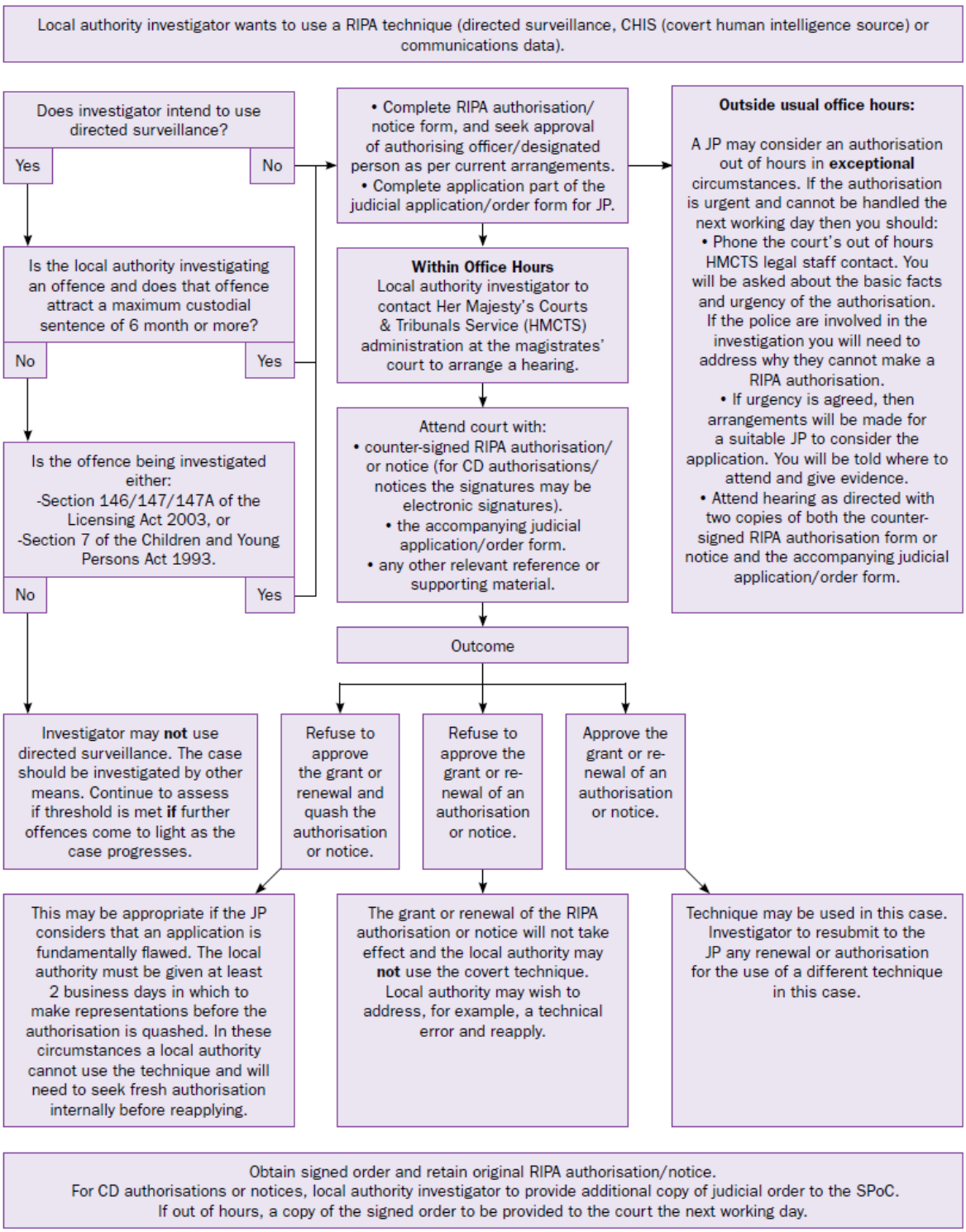


TABLE 2 - APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Appendix A – RIPA Forms

FORMS	TITLE	LINK
RIPA 1	Part II Application for Authorisation (Directed Surveillance).	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc
RIPA 2	Application for a Renewal of Authorisation for Surveillance	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/renewal-directed-surveillance
RIPA 3	Cancellation of Authorisation (Directed Surveillance).	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan
RIPA 4	Review of Authorisation (Directed Surveillance).	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/review-directed-surveillance
RIPA 5	Application for Communications Data	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/communications-data1.doc
RIPA 6	Notice Under Section 22(4) of the RIPA 2000 Receiving Communications Data to be Obtained and Disclosed	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/specimen-part-I-ch-II-notice
RIPA 7	Part II Application for Authorisation (CHIS).	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application
RIPA 8	Review of A covert human intelligence source (CHIS) authorisation.	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review
RIPA 9	Application for renewal of a covert human intelligence source (CHIS) authorisation	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal
RIPA10	Cancellation of an authorisation	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation

	for the use or conduct of a covert human intelligence source	
RIPA 11	Request schedule for subscriber information	http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/RIPAschedule-for-subscriber-info

Appendix B – Authorising Officers

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

***Notes:**

I. The Authorising Officer must be 'Operationally Independent' from any investigation they are asked to consider for approval. If this requirement cannot be shown to have been met OR if there is any uncertainty, then a different Authorising Officer who is independent, must consider the application.

II. For guidance, areas of investigation presumed to compromise respective Approving Officers operational independence are shown in the table below.

III. Ultimately it is for Approving Officers to make this judgment in each case. I.e. To ensure their Operational Independence AND their ability to demonstrate this to the IOCCO if required.

Designation	**Officer**	**Scope**	**Exclusions**
Chief Executive	John Gilbert	All purposes (including where there is a likelihood of acquiring confidential information)	Where there is insufficient Operational Independence
Head of Internal Auditor	Nick Hobbs	Any appropriate investigation	Fraud etc. Investigations
Head of Benefits	Andy Stevens	Any appropriate investigation.	Benefits etc investigations
Director of Law & Democratic Services	Stephen Taylor	Senior Responsible Officer.*	**Precluded*.
Board Director Service Delivery	Bernie Brannan	All purposes (including where there is a likelihood of acquiring confidential information, but only in the absence of the Chief Executive)	Where there is insufficient Operational Independence.

Designation	Officer	Scope	Exclusions
Public Protection Manager	Paul Simmonds	Environmental Crime and any other appropriate investigations. *Single Point of Contact for Acquiring Communications Data RIPA Coordinator*	Investigations involving: Environmental Health Trading Standards matters *(Including specific authorised 'Scambuster' operations)*
Head of Planning, Regulatory Services, Heritage & Libraries.	Richard Bell	Any appropriate investigation.	Investigations Involving: Planning Trees Licensing Taxis Animal welfare and related Offences.
Head of Housing Services	Michael Ash	Any appropriate investigation.	Housing Anti-Social Behaviour investigations.
Head of Commissioning Children's & Adults	Sue Wald	Any appropriate investigation.	Truancy Youth Offending Safeguarding and other related issues where there is insufficient operational independence.

**Explanation:*

The Government's recent legislative and policy changes to the Code of Practice for the Acquisition and Disclosure of Communications Data, which came into force in March 2015 requires relevant authorities to ensure the independence of the Designated Person (DP) and other RIPA Authorisers. The Code requires public authorities to satisfy IOCCO that they have sufficient measures in place to ensure independence.

Appendix C - Codes of practice

Covert Surveillance Code of Practice
https://www.gov.uk/government/publications/code-of-practice-for-covert-surveillance-and-property-interference

Covert Human Intelligence Code of Practice
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97958/code-practice-human-intel.pdf

Interception of Communications Code of Practice
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf

Investigation of Protected Electronic Information Draft Code of Practice (29/06/2007)
http://www.legislation.gov.uk/ukdsi/2007/9780110772455/note

Acquisition and Disclosure of Communications Data Code of Practice
https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)
Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

APPENDIX D

Specimen Directed Surveillance application form

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Sample Form with Notes To Assist Completion

This form is to be completed by an officer of the local authority seeking authorisation to carry out Directed Surveillance. If granted, authorisation will last for a period of up to three months.

Code of Practice: *References to the "Code" or "Code of Practice" are to the RIPA Covert Surveillance Code of Practice.*

Unique Reference Number (URN): *This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which are issued by the same department. The idea is that, during an OSC inspection, the inspector can see which forms relate to each other. A URN also allows the form relating to each investigation to be kept together in the Central Record. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. There are no hard and fast rules.*

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			

Investigation/Operation Name (if applicable)	
Investigating Officer (if a person other than the applicant)	

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171. [1]

Insert the name and position of the Authorising Officer. This is the person who will decide whether or not Directed Surveillance should be authorised and he/she will countersign this form.

2. Describe the purpose of the specific operation or investigation.

For example:

- *To investigate acts of crime or disorder e.g. racially aggravated criminal damage and racist verbal abuse*
- *To investigate and gather evidence of a potential benefit fraud*
- *To investigate instances of illegal dumping of waste*

If possible, include the relevant legislation that would be used to prosecute offenders and/or which gives you the power/duty to investigate the matter

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

The key phrase here is "in detail." Therefore a response, which merely states, "Video camera and recording equipment will be installed at a fixed point", will not be adequate.

Your statement here needs to include what is going to be done, who is going to do it, when they are going to do it, where they are going to do it and how they are going to do it. Other points to address here include:

- *How long will the surveillance last?*
- *Specific details about dates and times i.e. is it 24/7, at specific times of the day or at random times?*
- *Which premises are to be used and/or targeted?*
- *Which vehicles are to be used? Are they public or private?*
- *What type of equipment is to be used?*

Note that, if the Authorising Officer approves this surveillance, your authorisation will only cover you to do what you have stated here (subject to any amendments made by the Authorising Officer in box 12). Consequently you can only rely on section 27 "the RIPA Shield/Defence" only in so far as you were undertaking the activities set out in this section (as amended). Therefore it pays to include lots of detail.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

Include as much information as you have. If you do not know the identity say so. Other information could include a general description of the possible target(s).

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Your statement here should be more detailed than in Box 2. You should give details of the precise information sought by doing the surveillance. For example:

- *To ascertain what time the suspect enters and leaves the building*
- *Or to capture images of the perpetrators of anti social behaviour at (place/address)*
- *To find out who is delivering the goods to the suspect's premises etc (place/address)*

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on.(SI 2003 No.3171)*

- ~~*In the interests of national security;*~~
- ***For the purpose of preventing or detecting crime or of preventing disorder;***
- ~~*In the interests of the economic well-being of the United Kingdom;*~~
- ~~*In the interests of public safety;*~~
- ~~*for the purpose of protecting public health;*~~
  - ~~*for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;*~~

Since 5th January 2004, local authorities can only authorise Directed Surveillance for the purpose of preventing or detecting crime or of preventing disorder.

Therefore all other grounds should be deleted.

7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]

State why Directed Surveillance is needed to obtain the information that is sought.

The most important question to address is – why is it necessary to use covert surveillance?

How will doing the Directed Surveillance lead to prevention or detection of crime or prevention of disorder?

Factors to include will be:

- *The offence or disorder you are investigating*
- *Seriousness of the offence*
- *Impact on victims*
- *What other means you have tried/considered to obtain the information and why are those impracticable*

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]

Describe precautions you will take to minimise collateral intrusion

When doing Directed Surveillance you may be invading the privacy of those who are not your target e.g. third parties, passers by etc. RIPA requires you to think about their rights and what you can do to minimise the impact on them of your surveillance.

Paragraph 2.6 of the Code of Practice states:

"Before authorising surveillance the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation".

People who may be the subject of collateral intrusion include:

- *Customers or workers at a business premises*
- *Visitors to a property*
- *Friends or relatives of the suspect*

Firstly, identify here who else may be caught by the surveillance.

Secondly, state why it is unavoidable. This could be because of the nature of the premises (e.g. restaurant) or because of what the person is doing (e.g. visiting other subject/target premises) that there will always be third parties around who will be captured on film or whose activities will be recorded/observed in some way.

Thirdly set out what steps you have taken to minimise collateral intrusion. This may include:

- *Using a still camera as opposed to a video camera*
- *If installing hidden cameras, only switching them on at specific times rather than all the time*
- *Narrowing the field of vision or the place where the cameras are cited*
- *Reducing the amount of surveillance done at busy times e.g. shops or places of worship*

If you cannot minimise collateral intrusion you still need to show you have considered it. You may wish to add that you cannot do anything to minimise it but you will not be making any decisions on the information gathered about third parties unless it shows them committing a criminal offence.

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 2.5]

Paragraph 2.6 of the Code of Practice states:

"This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity 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. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair".

This requires you to justify the need for the surveillance and the methods used and balance those with the impact on the privacy of the subject. The DCA guide on Human Rights (page 55) states:

"When taking decisions that may affect any of the qualified rights, a public authority must interfere with the right as little as possible only going as far as is necessary to achieve the desired aim."

To demonstrate proportionality you must consider the following elements,

Is this use proposed use proportionate

- ***To the seriousness of the offence or the mischief***
- ***To the degree of intrusion on the target and other people***
- ***Have other overt means been considered and discounted***

the following issues must be addressed here

- *Can you get information using less intrusive means/other methods?*
- *What other means have you tried?*
- *What have you done to try and lessen the impact on the target? Factors to set out include:*
  - *Amount of information to be gathered during the surveillance*
  - *Impact of surveillance on the subject*

- *Timing of the surveillance*

At the same time, the above must be balanced with the need for the activity in operational terms. To demonstrate this balance you should set out:

- *What you are seeking to achieve?*
- *Seriousness of the offence*
- *Impact of the offence on the victims, others/wider community and on the public purse*

10. Confidential information. [Code paragraphs 3.1 to 3.12]

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

This is defined in the Code of Practice as communication involving confidential personal information (including health and religious counselling information), confidential journalistic material or communications subject to legal professional privilege.

Local authorities are unlikely to come across the kind of information during routine surveillance operations. However you have to be alive to the possibility and add include wording here to show how you have thought about it. For example, where you will be following someone who may end up at a church, mosque or doctor's surgery.

Note that in cases where you will be obtaining confidential information, the authorisation has to be granted by the Chief Executive or, in his/her absence, a chief officer.

11. Applicant's Details.

Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

This section is for the Authorising Officer to complete. It should not be pre completed by the investigating officer. Sufficient detail must be included here to demonstrate that he/she has considered thoroughly. Reference can be made to the boxes above but "cut and paste" should be avoided.

The five "Ws" stated above must be addressed in detail. This is important so that investigating officers are clear as to what they can and cannot do and the means that they can adopt. The Authorising Officer should not be afraid to reject the application if it lacks clarify or detail.

13. Explain why you believe the directed surveillance is necessary. [Code paragraph 2.4] **Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]**
You may refer to box 7 and 9 when completing this section. You can also add any additional factors you have considered. However, to demonstrate that you have given the issues due to thought, if it important not to cut and paste that wording or to just state "see box 7 and 9".

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 3.1 to 3.12	
This box should only be completed if you are likely to obtain Confidential Information (see box 10) through Direct Surveillance.	
Date of first review	
Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.	
Regular reviews are stressed by the Code of Practice. Where a surveillance operation is going to last more than one month then, the Surveillance Commissioners have suggested, there should be at least a review once a month. Shorter or time limited operations may not require a review. *During a review consideration will have to be given to whether the surveillance is still necessary and proportionate. A standard form is available to record the review.*	

Name (Print)		**Grade / Rank**		
Signature		**Date and time**		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]				

15. Urgent Authorisation [Code paragraphs 4.17 and 4.18]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.
Paragraph 4.13 of the Code of Practice states: *"A case is not normally to be regarded as urgent unless 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, by likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need to for an authorisation has been neglected or the urgency is of the authorising officer's own making."* *In urgent cases this section still has to be completed as soon as reasonably practicable. It will be rare for a local authority to be able to claim that an authorisation was so urgent that it had to be obtained verbally.*
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer
This section is only to be completed where an urgent verbal authorisation was given by an Authorising Officer only entitled to act in urgent cases. This will usually not be appropriate for local authorities.

Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		

Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

APPENDIX E

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

APPENDIX F

NAFN Court Hearing Guidance

You may already be familiar with making applications to the Magistrates for orders in connection with the investigation of offences. All courts have local practices and if the practice at your local court is different you should follow the local practice.

1. Before the hearing

Read through the authorisation and the application form for Judicial Approval thoroughly. You are welcome to amend the application form supplied by NAFN but the authorisation itself should not be amended once it has been approved by the Designated Person.

Ensure you have: **The original authorisation plus one copy.**
Two copies of the application for Judicial approval
One copy of the Court Order form.

Be prepared to explain everything to the Magistrate – remember they may never have seen an application like this before. Try and anticipate what questions the Magistrate might ask.

Check if it is necessary for your Head of Legal Services to authorise you to appear in Court.

Make sure the Court know you are coming in advance.

2. At the hearing

You should address the Magistrate as ‘Sir’ or ‘Ma’am’. They may be accompanied by a legal adviser who will be a lawyer. The public should not be present during the application. This is important because anything heard by the public might get back to the person you are investigating.

After introducing yourself you may be asked to swear an oath (or make an affirmation). This is a matter for the Magistrate’s discretion. In general it is necessary to be sworn in if what you say is going to be treated as formal evidence. If, however, what you say is a presentation about the authorisation then it is not strictly necessary for you to be sworn in. Leave this to the Magistrate. If you are asked to swear an oath you can choose to affirm

instead if you object to swearing on the Bible/Holy book. Legally there is no difference between an oath or an affirmation. It is a matter of your own personal preference/religious belief. Magistrates should be able to accommodate all religious requirements.

The Magistrate may not be familiar with RIPA. It is helpful if you offer to talk them through the application, or the entire authorisation. The Magistrate may not find this necessary but they will generally appreciate the offer.

3. If everything goes well

Ask the Magistrate to sign the order. You need to keep the original authorisation and the original signed order. The Magistrate keeps a copy of everything for the Court records. Ensure that the scanned signed application form and order are returned to NAFN.

4. If the Magistrate is not happy to approve the authorisation

In most cases it is likely that the Magistrate will be happy to approve the authorisation.

However, if the Magistrate is not happy to authorise try to get as much information as possible as to why. It might be helpful to ask them if there is any further information which can be provided in support to help persuade them in future. You cannot amend the authorisation without getting it approved again by the Designated Person, but you can amend the application for Judicial approval. You can also provide further evidence to the Magistrate outside the application – if they agree to this.

If the Magistrate considers quashing the authorisation they must adjourn the application for at least two working days to give you a chance to make further representations. Although this isn't in RIPA, it is a strict legal requirement in the Criminal Procedure Rules (rule 6.28).

Whatever the outcome you should take the original authorisation with you when you leave.

5. Need further advice

If you are not sure of what to do next or need further advice contact NAFN who will be able to assist and direct your query accordingly.

NAFN UK North NAFN UK South

Telephone: 0161 342 3727 **Telephone:** 01273 291322
Email: **spoc@nafn.scn.gov.uk** Email: **spoc@nafn.scn.gov.uk**

Version Control

Issue	Date	Purpose	Reviewed by	Approved by
1.0	April 03	Initial Draft	Geoffrey Snowball	Stephen Taylor
2.0	Nov 05	Amended procedures	Phil Thomas	Stephen Taylor
3.0	Mar 07	Amended procedures	Phil Thomas	Stephen Taylor
4.0	Oct 07	Amended procedures	Phil Thomas	Stephen Taylor
5.0	April 08	Amended procedures	Phil Thomas	Stephen Taylor
6.0	May 08	Amended procedures	Phil Thomas	Stephen Taylor
7.0	Jan 09	Amended procedures	Phil Thomas	Stephen Taylor
8.0	Mar 09	Amended procedures	Phil Thomas	Stephen Taylor
9.0	May 09	Amended procedures	Phil Thomas	Stephen Taylor
10.0	Oct 10	Amended procedures	Phil Thomas	Stephen Taylor
11.0	July 10	Amended procedures	Phil Thomas	Stephen Taylor
12.0	Aug 10	Amended procedures	Phil Thomas	Stephen Taylor
13.0	Feb 12	Amended procedures and authorisers in light of Council restructure	Phil Thomas	Stephen Taylor
14.0	Oct 12	Amended procedures in light of the changes to the RIPA procedures for Local Authorities	Philip Thomas	Stephen Taylor
15.0	Nov 14	Updated list of Authorisers and refresh of all hyperlinks to key Govt. documents and procedures. .	Paul Simmonds	Stephen Taylor
16.0	Nov 15	Update guidance and amend scope of Authorisers to ensure operational independence	Paul Simmonds	Stephen Taylor.