

WILTSHIRE COUNCIL

CORPORATE POLICY AND PROCEDURES DOCUMENT

ON

THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

INDEX

PAGE NO.

1.	Background	3
2.	Overview	3
3.	Definitions	4
4.	Authorisation Procedure	7
5.	Role of the Authorising Officer	8
6.	Considering an Application for a Surveillance Activity	11
7.	Authorising a CHIS	13
8.	Accessing Communications Data	14
9.	Working with / through Other Agencies	15
10.	Records Management	16

APPENDICES

Appendix 1	Authorisation Process Charts	17
Appendix 2	List of Authorising Officers	19
Appendix 3	List of Designated Persons and SPOCs	20

1. BACKGROUND

- 1.1 The Regulation of Investigatory Powers Act 2000 (RIPA), which came into force on 25 September 2000, was enacted in order to regulate the use of a range of investigative powers by a variety of public authorities. It gives a statutory framework for the authorisation and conduct of certain types of covert surveillance operation. Its aim is to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action.
- 1.2 It is consistent with the Human Rights Act 1998 and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights (right to respect for a person's private and family life, home and correspondence). Compliance with RIPA means that any conduct authorised under it is "lawful for all purposes". This important protection derives from section 27(1) of RIPA, which gives the authorised person an entitlement to engage in the conduct which has been authorised. Compliance with RIPA will assist the Council in any challenges to the way in which evidence has been gathered and will enable the Council to demonstrate that it has acted lawfully.
- 1.3 Compliance with RIPA makes authorised surveillance "lawful for all purposes" pursuant to section 27(1) of the Act. Compliance with RIPA will protect the Council from challenges to both the gathering of, and the subsequent use of, covertly obtained information. Non-compliance may result in:
 - (a) evidence being disallowed by the courts;
 - (b) a complaint of maladministration to the Ombudsman; or
 - (c) the Council being ordered to pay compensation.
- 1.4 It is essential therefore that the Council's policies and procedures, as set out in this document, are followed. A flowchart of the procedures to be followed appears at Appendix 1.

2. OVERVIEW OF POLICY

- 2.1 Authorisation must be applied for in the manner provided in section 4 of this policy when the Council undertakes any directed covert surveillance, uses a covert human intelligence source (CHIS) or wishes to access communications data. Authorisations for directed covert surveillance and for the use of a CHIS are made to Authorising Officers. Applications for access to communications data are made to a single point of contact (SPOC).
- 2.2 Authorising Officers are obliged to consider all applications they receive in accordance with sections 5 and 6 of this policy. When considering applications for the use of a CHIS, the Authorising Officer must consider the additional matters set out in section 7. An authorisation can only be granted where the surveillance activity is necessary for the detection or prevention of crime or for preventing disorder and the

Authorising Officer considers that covert surveillance is a proportionate way for the Council to obtain the desired information.

- 2.3 The accessing of communications data is governed by section 8 of this policy. Applicants wishing to obtain access to communications data must make an application to a SPOC, who will refer the application to a specified Designated Person. The Designated Person will determine whether to grant the application. If it is granted, the SPOC will liaise with the communications service provider in order to obtain the communications data requested.
- 2.4 Section 9 of this policy covers the arrangements for working with or through other agencies for surveillance purposes.
- 2.5 Section 10 of this policy sets out the requirements for records management. This includes both departmental records and the central record which is maintained by the Solicitor to the Council.

3. DEFINITIONS

Authorising Officers

- 3.1 Authorising Officers are senior officers of the Council who have received training in the application of RIPA. Only Authorising Officers have power to authorise directed surveillance and/or the use of a covert human intelligence source. Authorising Officers are listed at Appendix 2.

CHIS (Covert Human Intelligence Sources)

- 3.2 The conduct and use of a covert human intelligence source means in effect the use of an informant.
- 3.3 The conduct and use of a covert human intelligence source occurs when a person establishes or maintains a personal or other relationship with a person:
 - for the covert purpose of using the relationship to obtain information or to provide access to any information to another person; or
 - in order to disclose information covertly obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.
- 3.4 A person may be a CHIS if they induce, ask or assist another person to engage in the conduct described in paragraph 3.3 above.
- 3.5 RIPA does not apply in circumstances where members of the public volunteer information to the Council or to contact numbers set up to receive information.
- 3.6 Carrying out test purchases will not require the purchaser to establish a relationship with the supplier for the 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) although an Officer covertly watching a particular transaction may require an authorisation for directed surveillance.

- 3.7 By contrast, developing a relationship with a person in the shop, for example to obtain information about the seller's supplier of an illegal or unsafe product, will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is happening in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

Collateral Intrusion

- 3.8 Collateral intrusion is intrusion into the privacy of persons other than those who are directly the intended subjects of the investigation or operation.

Communications Data

- 3.9 Communications data means any information held or obtained by a telecommunications service or postal service that relates to a person. It includes any information held by those services about that person's use of those services.
- 3.10 Communications data does not include the content of any communications held by any telecommunications or postal service and nothing in this policy authorises Council officers to access such data.

Confidential Information

- 3.11 Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.
- 3.12 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. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

Designated Person

- 3.13 A Designated Person is a senior officer of the Council who has received training for the purpose of considering applications for access to communications data.
- 3.14 Designated Persons are listed at Appendix 3 of this policy.

Directed Surveillance

- 3.15 Directed Surveillance is surveillance which:-

- is covert;

- is not intrusive surveillance;
- is undertaken for the purpose of a specific investigation or operation;
- is undertaken in such a manner that it is likely that private information about an individual is obtained (whether or not that person is specifically targeted for the purposes of the investigation or operation); and
- is not carried out by way of an immediate response to events, which would make seeking authorisation under the Act reasonably impracticable.

Intrusive Surveillance

3.16 This is when surveillance:-

- is covert;
- relates to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of a person on the premises or in the vehicle or is carried out by means of a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises/vehicle will not be intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

3.17 This form of surveillance can be carried out only by the police and other law enforcement agencies. Council officers must not carry out intrusive surveillance.

Private Information

3.18 Private information in relation to a person includes any information relating to his/her private and family life, home and correspondence. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about that person and possibly others with whom he/she associates.

3.19 It is also likely that surveillance of a person's commercial or business activities will reveal information about his or her private life and the private lives of others. Authorisation may, therefore, be required where surveillance is focusing on business or commercial activities.

Single Points of Contact (SPOCs)

3.20 A single point of contact (SPOC) is a person who has received specific training in accessing communications data and who is named in this policy as one of the Council's SPOCs.

3.21 SPOCs are listed at Appendix 3 of this policy.

Surveillance

3.22 'Surveillance' includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- recording anything mentioned above in the course of authorised surveillance.
- Surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

Overt Surveillance

3.23 Surveillance will be overt if the act of surveillance is not calculated to be hidden from view, even if the motives of the person undertaking the surveillance remain concealed.

Covert Surveillance

3.24 Surveillance will be covert if it is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.

4. AUTHORISATION PROCEDURE

The need for authorisation

4.1 All Council officers must receive authorisation **in writing** before undertaking:

- (a) directed covert surveillance;
- (b) the conduct and use of a covert human intelligence sources; and/or
- (c) the accessing of communications data .

4.2 No Council officer may undertake any intrusive covert surveillance.

Making the application for authorisation

4.3 Applications to undertake the activities listed at paragraph 4.1 above must be made as follows:

- (a) All applications for authorisation to undertake directed covert surveillance must be made on form 1A.
- (b) All applications for authorisation to use a covert human intelligence source must be made on form 2A.
- (c) All applications for authorisation to access communications data must be made on form 3A and the procedure in section 8 of this policy must be followed.

- 4.4 Standard application forms are held by the Legal Unit and can be obtained from the Intranet.
- 4.5 With the exception of applications for authority to access communications data, all applications must be sent to the relevant departmental Authorising Officer listed in Appendix 2. Applications for access to communications data must be made to one of the SPOCs listed in Appendix 3.

Authorisation in urgent cases

- 4.6 In urgent cases, an oral application for authorisation may be made but only if the time that would elapse before a written authorisation could be granted would be likely to endanger life or jeopardise the investigation or operation to which the authorisation relates.
- 4.7 An authorisation will not be urgent where the need for authorisation has been neglected or is of the officer's own making.
- 4.8 An urgent authorisation lasts no more than 72 hours and is granted orally but must be recorded in writing as soon as possible. A written application for authorisation must be made before the expiry of the urgent authorisation.

Applying for renewal

- 4.9 An officer who has received an authorisation is responsible for renewing that authorisation if the activity for which authorisation was given is expected to continue beyond the duration of the authorisation. Renewal applications should be made before the initial authorisation expires. If necessary a renewal can be granted more than once.
- 4.10 Applications for renewal of an authorisation for directed covert surveillance must be made on form 1C. Applications for renewal of an authorisation for use of a covert human intelligence source must be on form 2C. All renewal applications must be made to the Authorising Officer who granted the initial authorisation.

Cancelling an authorisation

- 4.11 The officer responsible for undertaking the authorised surveillance must apply to have that authorisation cancelled when the investigation or operation for which authorisation was given has ended, the authorised surveillance activity has been completed, or the information sought is no longer necessary.
- 4.12 An application for cancellation must be made on form 1D for a directed covert surveillance authorisation or form 2D for a covert human intelligence source authorisation. An application to cancel an authorisation to access communications data is made on form 3D and is governed by paragraphs 8.11 – 8.13 of this policy.
- 4.13 **No authorisation can be left to expire.** All authorisations, apart from authorisations to access communications data, must either be renewed, if the surveillance is expected to continue beyond the duration of the authorisation, or cancelled, if the surveillance ends before the expiry date.

Authorising Officers

- 4.14 The officers who can give authorisation for directed surveillance or for the conduct and use of a CHIS are listed in Appendix 2. The officers who can grant authorisations for access to communications data are listed in Appendix 3.

5. ROLE OF THE AUTHORISING OFFICER

Considering and granting authorisations

- 5.1 Authorising Officers are responsible for receiving, considering and, where appropriate, granting applications for authorisation. Authorising Officers should follow the steps set out in section 6 below when considering applications for authorisation.
- 5.2 An Authorising Officer is not empowered to consider an application for access to communications data. Where such an application is received by an Authorising Officer, it must be referred to one of the SPOCs listed in Appendix 3 and applicant must be informed.
- 5.3 An Authorising Officer is empowered to grant urgent authorisations where appropriate, to renew authorisations and to cancel authorisations. Authorising Officers should also review all authorisations he or she has granted from time to time.
- 5.4 An Authorising Officer cannot delegate their power to authorise surveillance under RIPA to anyone else.

Urgent authorisations

- 5.5 Authorising Officers are responsible for issuing urgent authorisations where appropriate. In exceptional circumstances, an urgent authorisation may be given orally if the time that would elapse before a written authorisation could be granted would be likely to endanger life or jeopardise the investigation or operation to which the authorisation relates.
- 5.6 An authorisation will not be urgent where the sudden need for authorisation is due to the neglect of the Officer or is otherwise of the Officer's own making.
- 5.7 The officer to whom urgent authorisation is given must make a written application for retrospective authorisation within 72 hours of the urgent authorisation being given.
- 5.8 All urgent authorisations must be recorded immediately on the central register together with the date and time of the authorisation.

Duration

- 5.9 An Authorising Officer can grant a standard written authorisation for directed surveillance or for the conduct and use of a CHIS for any time period up to three months.

- 5.10 In the case of an urgent application, an oral authorisation can be given for up to 72 hours and a written application must be made before the expiry of that time limit.

Periodic review

- 5.11 An Authorising Officer should conduct regular reviews of authorisations granted in order to assess the need for the authorised activity to continue. The Authorising Officer shall determine how often a review should take place. Authorisations should be reviewed frequently where the surveillance involves collateral intrusion (i.e. relating to other people who are not targets but who may be affected by the operation) or provides access to confidential information.
- 5.12 Reviews must be completed on form 1B in respect of an authorisation for directed covert surveillance and form 2B for the conduct and use of a covert human intelligence source. A review necessarily involves consultation with the persons involved in the surveillance activity. The Applicant must give sufficient information about the product of the surveillance for the Authorising Officer to be satisfied that the authorised activity should continue.
- 5.13 An Authorising Officer must cancel the authorisation if, as the result of a review, he or she is of the opinion that the grounds for granting the authorisation no longer apply.
- 5.14 The results of all reviews must be recorded in the central record of authorisation.

Granting a renewal

- 5.15 Renewal applications should be made by the officer who applied for the initial authorisation.
- 5.16 When receiving a renewal application, the Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred. The Authorising Officer must be satisfied that it is necessary and proportionate for the authorisation to continue.
- 5.17 An authorisation may be renewed before the initial authorisation ceases to have effect but the renewal takes effect from the time at which the authorisation would have expired. If necessary a renewal can be granted more than once.

Cancelling an authorisation

- 5.18 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting the authorisation no longer apply or if the authorisation is no longer necessary or proportionate. For instance, the authorisation should be cancelled if the aims have been met or if the risks have changed.
- 5.19 An authorisation can be cancelled on the initiative of the Authorising Officer following a periodic review, or after receiving an application for cancellation from the officer responsible for the surveillance activity.
- 5.20 All cancellation decisions made by an Authorising Officer must be recorded on form 1D for directed covert surveillance authorisations and form 2D for covert human intelligence source authorisations.

6. CONSIDERING AN APPLICATION FOR A SURVEILLANCE ACTIVITY

- 6.1 This part of the policy lists the factors which an Authorising Officer should consider upon receiving an application for an authorisation for directed surveillance, the use of a CHIS or a request to access communications data.

Step 1: Is an authorisation needed for this activity?

- 6.2 An Authorising Officer must first consider whether an authorisation is actually required. To require authorisation, the activity to which the application relates must be covert and must involve the obtaining of private information on an individual through either directed surveillance or the use of a CHIS.
- 6.3 An Authorising Officer should interpret the definitions broadly when determining whether an activity is covert or if private information will be obtained. When in doubt, the authorisation procedure must always be followed.
- 6.4 At no time can an Authorising Officer authorise any intrusive surveillance.

Step 2: Has the application been made on the correct form?

- 6.5 If the surveillance involves the use of an undercover person then a CHIS application must be made and the directions in section 7 of this policy considered in addition to this authorisation procedure.
- 6.6 If the surveillance involves accessing communications data, the Authorising Officer must refer the application to a SPOC and inform the applicant that the matter is now being considered in accordance with part 8 of this policy.

Step 3: Is the activity necessary?

- 6.7 An Authorising Officer can only authorise an activity that is necessary in the circumstances of the particular case if it is for the purpose of preventing or detecting crime or of preventing disorder. The Authorising Officer must be satisfied that there are no other reasonable means of carrying out the investigation, or obtaining the desired information, without undertaking the activity for which authorisation is sought.
- 6.8 Authorisation should not be granted if the information sought can be obtained by other means without undertaking an activity which falls under the requirements of RIPA. Authorisation cannot be granted if it is for any purpose other than the prevention or detection of crime or for the prevention of disorder.

Step 4: Is it proportionate?

- 6.9 Once satisfied that the activity is necessary, the Authorising Officer must then determine whether the activity is proportionate to what is sought to be achieved.
- 6.10 An Authorising Officer should first consider the following three primary factors in determining whether the activity for which authorisation is sought is proportionate:

6.10.1 Confidential Information

The Authorising Officer must take into account the likelihood of confidential information being acquired. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

Where confidential information is likely to be acquired, authorisation should only be given in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

In these circumstances, the Authorising Officer must be the Head of Paid Service or his deputy, as listed in Appendix 2.

6.10.2 Use of vulnerable persons as CHIS

When considering applications for the use of a CHIS, an Authorising Officer must determine whether the CHIS is a vulnerable individual or a juvenile in accordance with part 7 of this policy.

Where the proposed activity involves the use of a vulnerable person or juvenile as a CHIS, only the Head of Paid Service or his deputy as listed in Appendix 2 can give authorisation.

6.10.3 Risk of Collateral Intrusion

The Authorising Officer must consider whether there is a risk of collateral intrusion into the private life of any person not the primary subject of the investigation. The applicant should describe the activity sufficiently widely to include not only named individuals but also any others who may be at risk of collateral intrusion to enable this consideration to occur.

Where the risk of such intrusion is sufficiently significant, the Authorising Officer must determine whether a separate authorisation is required in respect of these other persons.

The person carrying out the activity must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then consider whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

6.11 The following further considerations must then be considered in determining whether the activity for which authorisation is sought is proportionate:

- Where the application is for the use of a CHIS, whether the safeguards and considerations listed in section 7 will be met;
- The reasons given by the applicant as to why that activity is sufficient and adequate for obtaining the information sought;

- Whether there are any other reasonable means of obtaining the information sought;
 - Whether the surveillance is an essential part of the investigation;
 - The type and quality of the information the activity will produce and its likely value to the investigation;
 - The amount of intrusion, other than collateral intrusion, the activity will cause and whether there are ways to minimise that intrusion; and
 - The length of time for which the authorisation is sought and whether the activity can be undertaken within a shorter time frame.
- 6.12 The Authorising Officer should only authorise the activity that is the least intrusive in the circumstances. Any unnecessary intrusion, including collateral intrusion, must be minimised as much as practically possible. **The least intrusive method will be considered proportionate by the courts.**
- 6.13 The Authorising Officer must balance 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 Authorising Officer should discuss the proposed activity, and any proposed changes, with the applicant prior to issuing the authorisation.

7. AUTHORISING A CHIS

- 7.1 When authorising the conduct or use of a CHIS, the tests set out in section 6 will still apply. However the Authorising Officer must also take into account the provisions of section 29 of RIPA and the Source Records Regulations (2000 SI No. 2725) made under it before authorising the conduct or use of a CHIS.
- 7.2 Section 29(5) requires the Authorising Officer to be satisfied that arrangements are in place for the careful management of the source and that records are maintained relating to the source which contain the particulars specified in the Source Records Regulations.
- 7.3 The Authorising Officer must therefore:
- (a) be satisfied that the conduct and/or use of the CHIS is both necessary and proportionate to what is sought to be achieved. This will be addressed by following the procedure provided in part 6;
 - (b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. This must address health and safety issues through a risk assessment;
 - (c) consider the likely degree of intrusion of all those potentially affected;
 - (d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

- (e) ensure records contain specified particulars relating to the source and that the records are kept confidential.

Vulnerable Individuals and Juveniles

- 7.4 Special safeguards apply to the use or conduct of vulnerable individuals or juveniles. 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 may need protecting from exploitation. A vulnerable individual will only be authorised to act as a source in the most exceptional circumstances.
- 7.5 A juvenile is a young person under 18. Juveniles can only be authorised as sources for one month. On no occasion can a child under 16 years of age be authorised to give information against his or her parents or anyone with parental responsibility for that child.
- 7.6 For both vulnerable individuals and juveniles, only the Head of Paid Service or his deputy can give authorisation (see Appendix 2).

8. ACCESSING COMMUNICATIONS DATA

The Application

- 8.1 A Council officer who wants to access communications data on a specific entity must make an application for access to communications data on form 3A and forward it to one of the Council's Single Points of Contact (SPOC), who are listed in Appendix 3 to this policy. The application process is described in Appendix 1C.

The Role of the SPOC

- 8.2 On receipt of an application for access to communications data, a SPOC shall assess the application for errors and assess whether the acquisition of specific communications data from a communications service provider (CSP) ought reasonably to be considered by a Designated Person. If the SPOC is of the opinion that the application is not necessary or proportionate, or is defective for any reason, the SPOC shall reject the application and return it to the applicant together with a completed form 3B.
- 8.3 If the SPOC is of the opinion that the application ought properly to be considered by a Designated Person, the SPOC shall complete the "request notice" in form 3C to accompany the application.
- 8.4 The SPOC shall then forward the authorisation and the request notice to the Designated Person to consider. During the consideration period the SPOC shall:
 - (a) advise the applicant and the Designated Person on the interpretation of the Act if required;
 - (b) provide assurance to the Designated Person that authorisations and notices are lawful under the Act and free from errors; and

- (c) assess any cost and resource implications, if appropriate, to both the public authority and the CSP of the data requirements.

8.5 Should the Designated Person grant an authorisation and return the authorisation and the request notice to the SPOC in accordance with the provisions below, the SPOC shall:

- (a) advise the applicant that the authorisation has been granted;
- (b) serve the request notice on the CSP requesting the communications data;
- (c) liaise with the CSP in order to obtain the communications data required; and
- (d) provide the communications data to the applicant once it is received.

The role of the Designated Person

8.6 A Designated Person shall consider all applications for authorisation to access communications data in accordance with part 6 of this policy. Authorisation to access communications data can only be granted if that access is necessary for the purpose of detecting or preventing crime or for preventing disorder. The authorisation must also be proportionate when considered in the context of the investigation.

8.7 For every application considered, the Designated Person shall record their decision and their reasons for it on the space provided on the application form.

8.8 A Designated Person shall have all the powers, obligations and responsibilities specified in part 5 of this policy in relation to authorisations for access to communications data, with the following exceptions:

- (a) Authorisations and notices for access to communications data can only be issued for a maximum time period of one month; and
- (b) Where urgent authorisation has been given orally, a written application must be made to the SPOC within one day of the oral authorisation being given.

8.9 If the Designated Person grants an authorisation to access communications data, he or she shall forward the authorisation, together with the request notice, to the SPOC.

8.10 There is no obligation to review an authorisation for communications data.

Cancelling an authorisation to access communications data

8.11 The Designated Officer must cancel an authorisation for access to communications data if the information is no longer necessary or the obtaining of it is no longer proportionate to the operation. To cancel an application, the applicant must complete form 3D and forward it to the SPOC who received the original application.

- 8.12 Should a SPOC receive an application to cancel an authorisation on form 3D, then the SPOC shall complete the SPOC portion of the cancellation notice that he or she has received and forward the cancellation notice to the Designated Person.
- 8.13 Should the Designated Person authorise the cancellation of the authorisation and forward the completed cancellation notice to the SPOC who shall subsequently:
- (a) prepare a “notice cancellation” in form 3E and send that form to the CSP, and
 - (b) orally advise the CSP to cease the collating and/or provision of any requested communications data

9. WORKING WITH/THROUGH OTHER AGENCIES

- 9.1 Where Council officers undertake an investigation/operation under RIPA jointly with another public authority, it is the responsibility of the tasking authority to obtain the authorisation. For example, if the Council was asked by the police to assist in a covert surveillance operation, the police should obtain the authorisation, which would then cover the Council.
- 9.2 In such a case, Council officers must request written confirmation from the other public authority that an authorisation is in place before taking part in any joint operation.
- 9.3 Likewise Council officers must ensure that they have authorisation to cover other public authorities where the Council has initiated a joint operation and be prepared to provide a copy of the authorisation where appropriate.
- 9.4 When an agency is instructed on behalf of the Council to undertake any action under RIPA, the Council instructing officer must obtain authorisation for the action to be undertaken and keep the agent informed of the various requirements. It is essential that the agent is given explicit instructions on what they are authorised to do.

10. RECORDS MANAGEMENT

- 10.1 The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in the relevant departments. A Central Record of all authorisation forms, whether authorised or rejected, will be maintained and monitored by the Solicitor to the Council.
- 10.2 All Authorising Officers and Designated Persons must send all **original** applications for authorisation to the Solicitor to the Council (fao Head of Legal Services). Each document will be given a unique reference number, a copy will be placed on the Central Record and the original will be returned to the applicant.
- 10.3 Copies of all other forms used must be sent to the Solicitor to the Council (fao Head of Legal Services) bearing the reference number previously given to the application to which it refers.

Departmental Records

10.4 Each department must keep a written record of all authorisations issued to it, to include the following:

- A copy of the application and authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the Authorising Officer;
- A record of the result of each review;
- A copy of any renewal of an authorisation and any supporting documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the Authorising Officer, including cancellation of such authorisation.

Central Record Maintained by the Solicitor to the Council

10.5 A central record of all authorisation forms, whether authorised or rejected, is kept by the Solicitor to the Council. The central record must be readily available for inspection on request by the Office of Surveillance Commissioners.

10.6 The central record must be updated whenever an authorisation is granted, renewed or cancelled. Records will be retained for a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive, or for such other period as determined by the internal procedures relating to the retention of the criminal or civil proceedings file.

10.7 The central record must contain the following information:

- The type of authorisation;
- The date on which the authorisation was given;
- Name/rank of the Authorising Officer;
- The unique reference number (URN) of the investigation/operation. This will be issued by the Legal Unit when a new application is entered in the Central Record. The applicant will be informed accordingly and should use the same URN when requesting a renewal or cancellation;
- The title of the investigation/operation, including a brief description and names of the subjects, if known;
- Whether urgent authorisation was given and why;
- If the authorisation was renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer;

- Whether the investigation/operation is likely to result in the obtaining of confidential information;
- The date and time that the authorisation was cancelled.

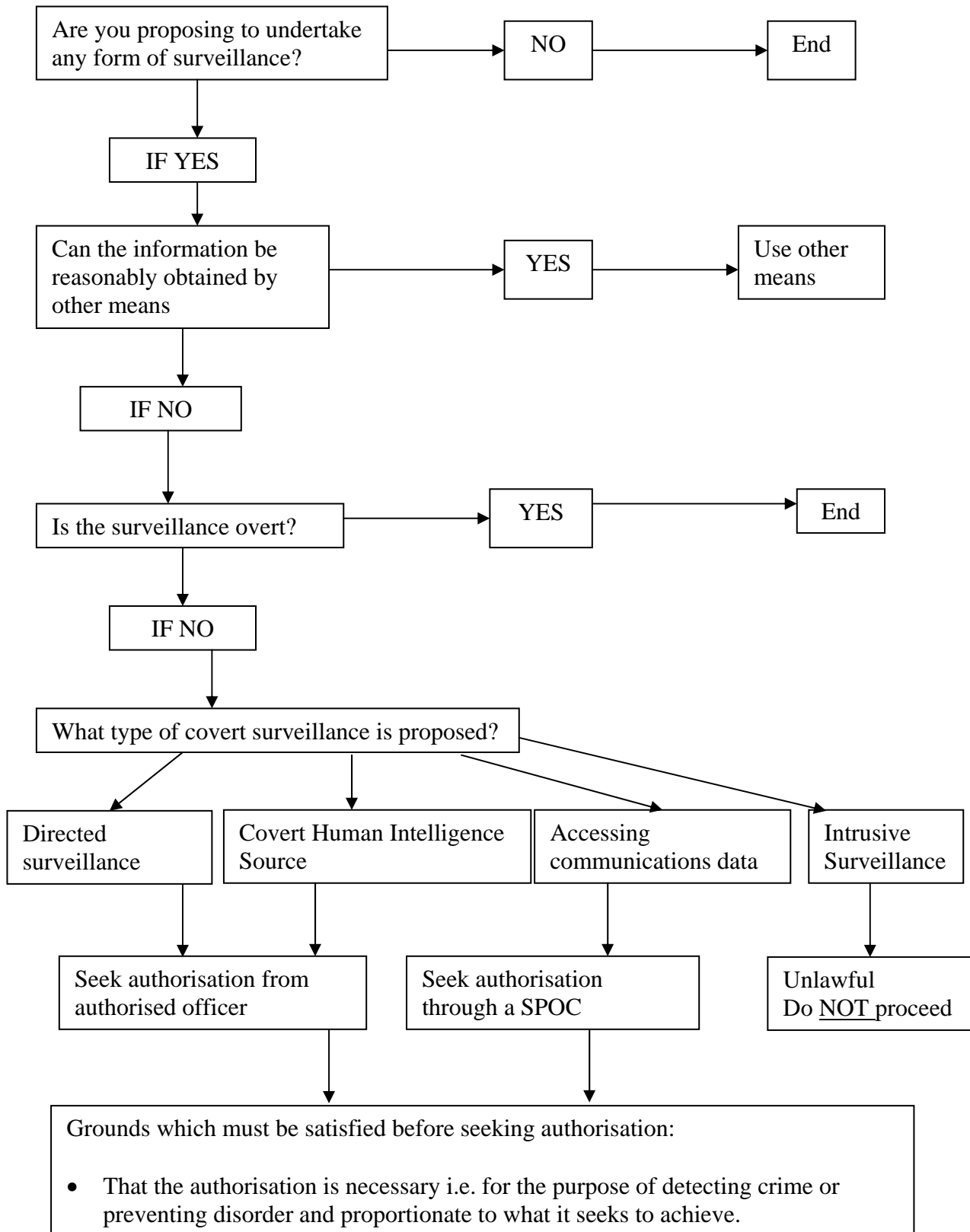
Retention and Destruction of Material

10.8 Departments must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Confidential material must be destroyed as soon as it is no longer necessary. It must not be retained or copied unless it is necessary for a specified purpose. Where there is doubt, advice must be sought from the Solicitor to the Council.

Policy updated September 2009

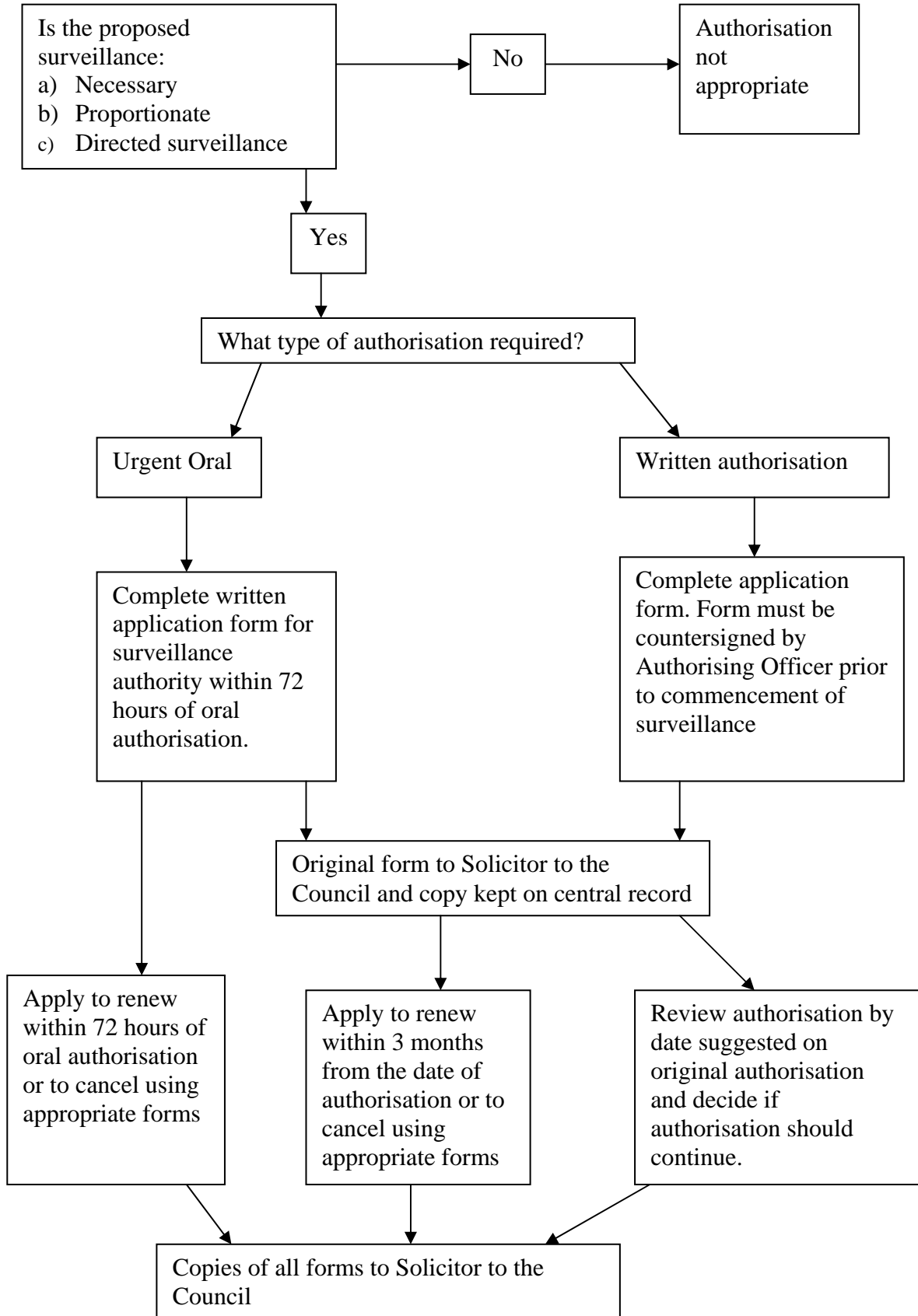
APPENDIX 1A

Do you need a RIPA authorisation?



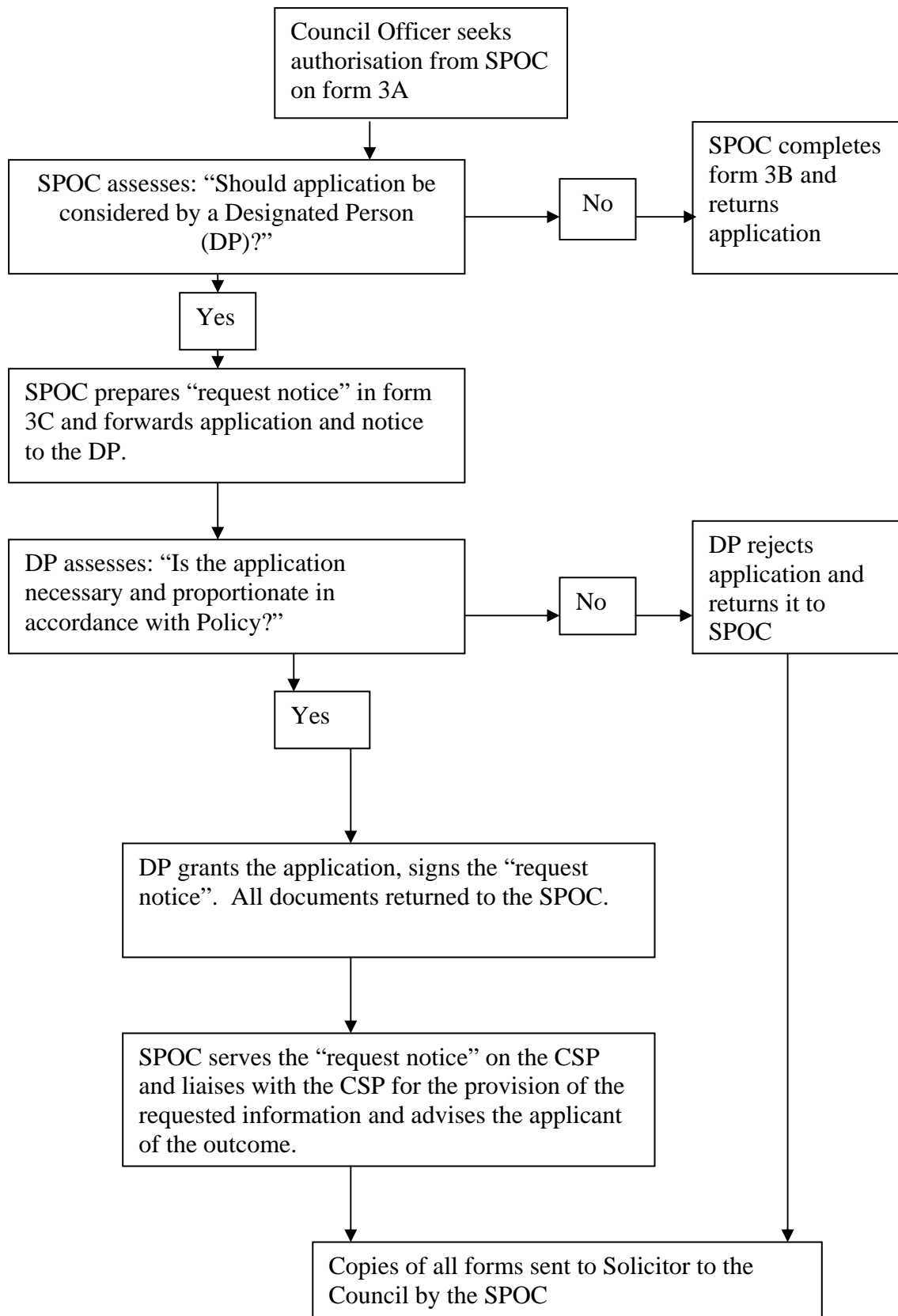
APPENDIX 1B

RIPA Authorisation Process for Directed Surveillance



APPENDIX 1C

Application Process for Authorisation to Access Communications Data



APPENDIX 2

List of Authorising Officers

1. For standard or urgent oral authorisations:

Where it is not likely that confidential information will be acquired

Department of Resources

- Ian Richard Gibbons, Solicitor to the Council and Monitoring Officer
- Julie Higginbotham, Head of Revenue and Benefits (North Hub)

Department for Children and Education

- Richard Parker, Service Director – Resources
- Maggie McDonald, Complaints Manager

Department of Transport, Environment and Leisure (TEL)

- Mark Smith, Service Director – Amenities and Leisure
- Alan Feist, Service Director – Sustainable Transport
- Tracy Carter, Service Director - Operations
- Steve Clover, Head of Commercial and Consumer Protection
- John Carter, Head of Environmental Protection and Licensing
- Steve Bowcock, Operational Team Leader, Waste Recycling and Cleaning

Department of Economic Development, Planning and Housing

- Mark Boden, Director of EDPH
- Gary Tomsett, Environmental Protection Specialist Team Manager
- Derek Streek, Head of Housing Management, South Wiltshire

2. For authorisations where it is likely that confidential information will be acquired or where using a CHIS who is a juvenile (under 16) or a vulnerable individual

- Dr. Keith Robinson, Head of Paid Service/Chief Executive

In his absence:

- Ian Richard Gibbons, Solicitor to the Council and Monitoring Officer

APPENDIX 3

List of Designated Persons

Designated Persons consider applications for access to communications data.

The Council's Designated Persons are in the Department of Transport, Environment and Leisure (TEL) and are as follows:

- Steve Clover, Head of Commercial and Consumer Protection
- Tracy Carter, Service Director - Operations

List of SPOCs

SPOCs receive and manage applications for access to communications data as well as liaising with communications service providers for the provision of that information.

The Council's SPOCs are in the Department of Transport, Environment and Leisure and are as follows:

- Yvonne Bennett, Consumer Protection Manager (North/West Hub), Economic Development, Planning and Housing
- John Devlin, Consumer Protection Manager, (East/South Hub), Economic Development, Planning and Housing