WILTSHIRE COUNCIL

CORPORATE POLICY AND PROCEDURES DOCUMENT

ON

ACCESSING COMMUNICATIONS DATA

(THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA))

INDEX PAGE NO.

1. BACKGROUND

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.

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.

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.

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

Authorisation must be applied for in the manner provided in section 5 of this policy.

Applicants wishing to obtain access to communications data must make an application to a Single Point of Contact (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.

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 Designated Person considers that the activity is a proportionate way for the Council to obtain the desired information.

Designated Persons are obliged to consider all applications they receive in accordance with section 6 of this policy.

Section 7 of this policy covers the arrangements for working with or through other agencies for surveillance purposes.

Section 8 of this policy sets out the requirements for records management. This includes both departmental records and the central record which is maintained by the Senior Responsible Officer.

3 OVERSIGHT OF THE POLICY

The Senior Responsible Officer is responsible for the integrity of the process within Wiltshire Council to authorise use of Covert Human Intelligence Sources (CHIS), compliance with Part II of the 2000 Act, Part III of the 1997 Act and with the Code of Practice, engagement with the Commissioners and Inspectors when they conduct their inspections and where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.

The Senior Responsible Officer shall also be responsible for ensuring 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 standard of authorising officers, the Senior Responsible Officer will be responsible for ensuring the concerns are addressed.

The Cabinet Member for Resources shall be responsible for ensuring that RIPA is being used consistently with this policy and that the policy remains fit for purpose. The Senior Responsible Officer shall provide a report on Wiltshire Council's use of RIPA to the Cabinet Member for Resources on a quarterly basis. A summary of this report shall be made available to all members of the Council. Annually, the report shall include a review of the effectiveness of this policy and any recommendation for changes to be made.. Any significant amendments to the policy shall be referred to the Cabinet for approval.

For the avoidance of doubt the Cabinet and the Cabinet Member for Resources are not to be involved in making decisions on specific authorisations.

4. DEFINITIONS

Cabinet

This is the body defined in Article 7 of the Wiltshire Council Constitution.

Collateral Intrusion

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

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.

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

Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

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

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.

Designated Persons are listed at Appendix 2 of this policy.

Private Information

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.

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.

Senior Responsible Officer

The Head of Legal Services, Wiltshire Council.

Single Points of Contact (SPOCs)

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.

SPOCs are listed at Appendix 2 of this policy.

5. AUTHORISATION PROCEDURE

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 2 to this policy. The application process is described in Appendix 1B.

The Role of the SPOC

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.

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.

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.

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

A Designated Person shall consider all applications for authorisation to access communications data in accordance with section 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.

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

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.

Duration of authorisations

Authorisations and notices for access to communications data can only be issued for a maximum time period of one month

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

Urgent Authorisations

In exceptionally urgent circumstances where authorisation has been given orally, a written application must be made to the SPOC within one day of the oral authorisation being given.

Cancelling an authorisation to access communications data

The Designated Person 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.

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.

Should the Designated Person authorise the cancellation of the authorisation and forward the completed cancellation notice to the SPOC, the SPOC 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

6. CONSIDERING APPLICATIONS TO ACCESS COMMUNICATIONS DATA

This part of the policy lists the factors which a Designated Person should consider upon receiving an application for an authorisation to access communications data.

Step 1: Is the activity necessary?

A Designated Person can only authorise an activity where s/he believes that the authorisation is necessary in the circumstances of the particular case for the purpose of preventing or detecting crime or of preventing disorder.

The Designated Person 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.

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 2: Is it proportionate?

If the activity is necessary, the Designated Person must also believe that the activity is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the activity against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the particular circumstances or if the information sought could reasonably be obtained by less intrusive means. Any activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Any conduct that is excessive in the circumstances of both the interference and the aim of the investigation or operation, or is in any way arbitrary will not be proportionate.

A Designated Person should first consider the following primary factors in determining whether the activity for which authorisation is sought is proportionate:

Confidential Information

The Designated Person 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.

Risk of Collateral Intrusion

The Designated Person 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 Designated Person must determine whether a separate authorisation is required in respect of these other persons.

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

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

- 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.

The Designated Person 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.**

The Designated Person 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 Designated Person should discuss the proposed activity, and any proposed changes, with the applicant before deciding on whether to authorise the activity

7. WORKING WITH/THROUGH OTHER AGENCIES

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. 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.

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.

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.

8. RECORDS MANAGEMENT

The Council must keep a detailed record of all authorisations, reviews, renewals, cancellations and rejections in the relevant services. A central record of all authorisation forms, whether authorised or rejected, will be maintained and monitored by the Senior Responsible Officer.

All Designated Persons must send all **original** applications for authorisation to the Senior Responsible Officer. 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.

Copies of all other forms used must be sent to the Senior Responsible Officer bearing the reference number previously given to the application to which it refers.

Service Records

Each service 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 Designated Person;
- A record of the period over which the surveillance has taken place;
- 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 Designated Person, including cancellation of such authorisation.

Central Record Maintained by the Senior Responsible Officer

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

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.

The central record must contain the following information:

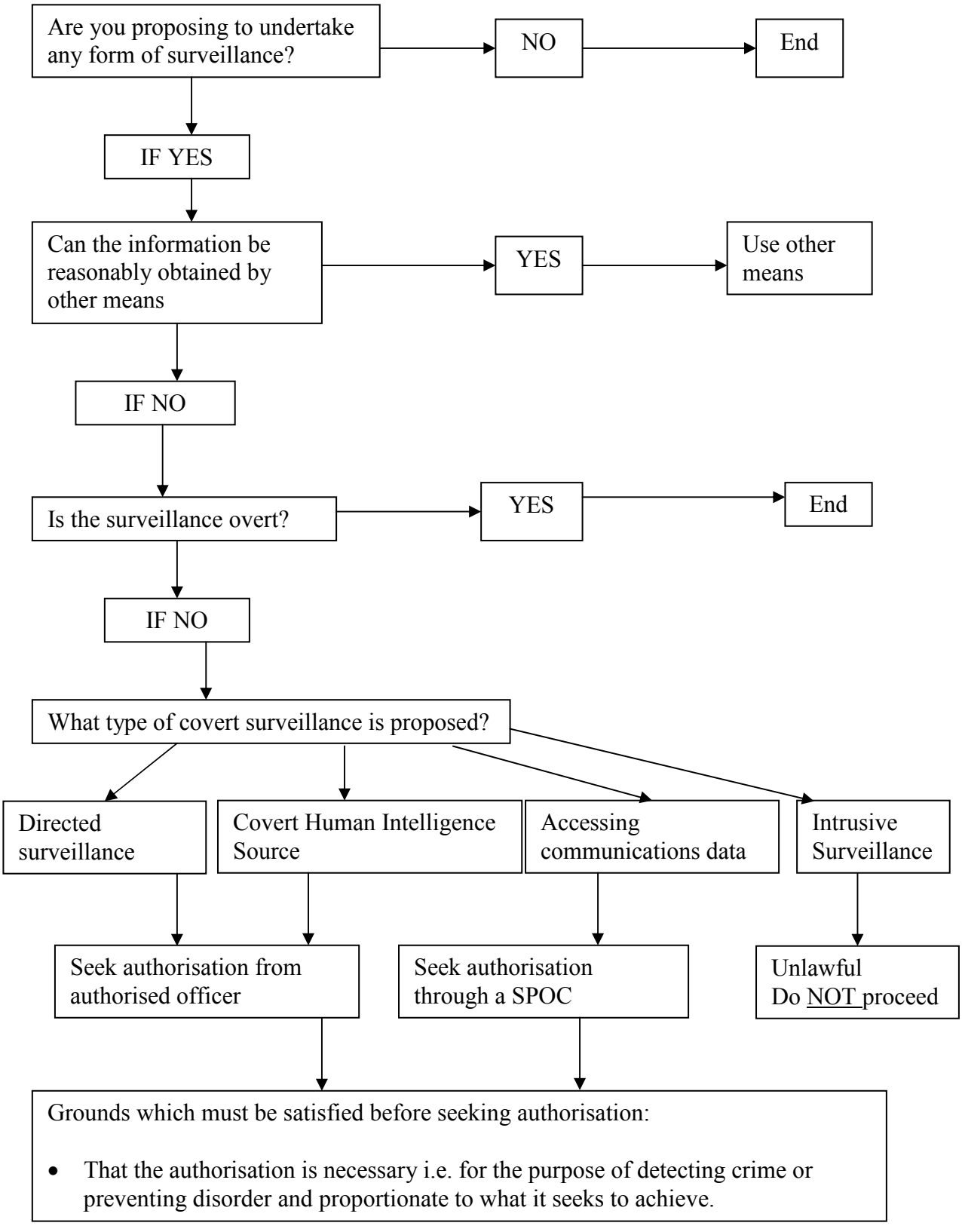
- The type of authorisation;
- The date on which the authorisation was given;
- Name/rank of the Designated Person;
- The unique reference number (URN) of the investigation/operation. This will be issued by the Legal Unit when a new application is entered in the Central Record. The applicant will be 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 Designated Person.
- 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

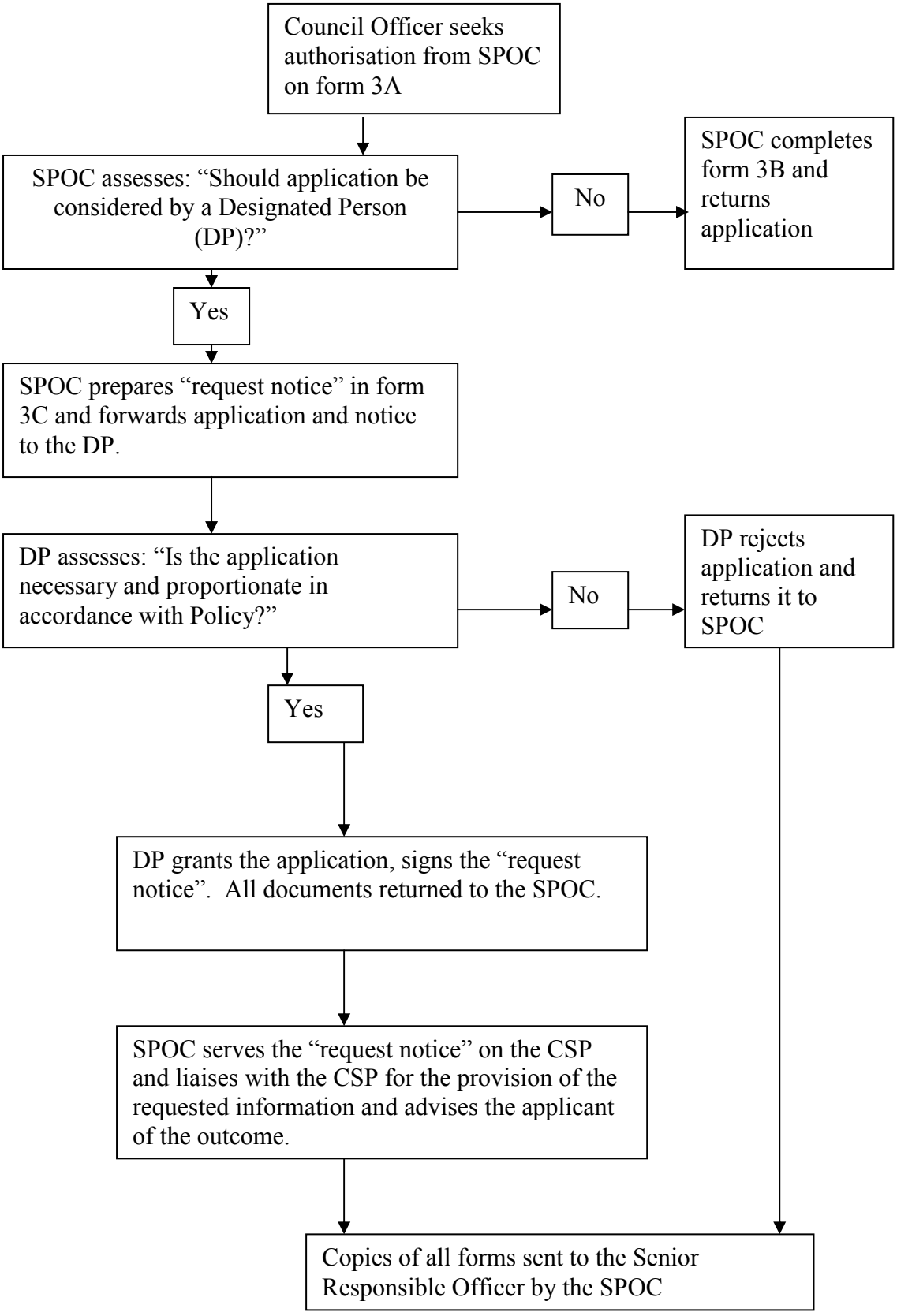
Departments must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Confidential material must be destroyed as soon as it is no longer necessary. It must not be retained or copied unless it is necessary for a specified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

APPENDIX 1A

Do you need a RIPA authorisation?



Application Process for Authorisation to Access Communications Data



APPENDIX 2

List of Designated Persons

Designated Persons consider applications for access to communications data.

The Council's Designated Persons are as follows:

- Steve Clover, Head of Commercial & Consumer Protection, Department of Public Health and Public Protection

- Tracy Carter, Service Director, Waste Management Services, Department of Neighbourhood and Planning

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 as follows:

- Yvonne Bennett, Consumer Protection Manager (North/West Hub), Department of Public Health and Public Protection

- John Devlin, Consumer Protection Manager, (East/South Hub), Department of Public Health and Public Protection