WILTSHIRE COUNCIL

CORPORATE POLICY AND PROCEDURES DOCUMENT

ON

DIRECTED SURVEILLANCE

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

INDEX PAGE NO.

1.	Background	3
2.	Overview	3
3.	Oversight of the Policy	4
4.	Definitions	4
5.	Authorisation Procedure	6
6.	Role of the Authorising Officer	7
7	Applications for Authorisations	9
8	Considering Applications for Directed Surveillance	10
9	Working With/Through Other Agencies	12
10.	Records Management	12

APPENDICES

Appendix 1	Authorisation Process Charts	14
Appendix 2	List of Authorising Officers	16
Appendix 3	List of Designated Persons and SPOCs	17

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. Applications for directed covert surveillance are made to Authorising Officers.

All Officers making applications and Authorising Officers should be aware of and familiar with the Home Office Covert Surveillance and Property Interference Revised Code of Practice (2010) or any code of practice issued in replacement of this code of practice.

Authorising Officers are obliged to consider all applications they receive in accordance with sections 6 and 8 of this policy 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.

Section 9 of this policy covers the arrangements for working with or through other agencies for surveillance purposes.

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 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 directed surveillance, 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

Authorising Officers

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. Authorising Officers are listed at Appendix 2.

Cabinet

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

Code of Practice

Home Office Covert Surveillance and Property Interference Revised Code of Practice (2010) or any code of practice issued in replacement of this code

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.

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.

Directed Surveillance

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

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.

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, nor enter on or interfere with property or wireless telegraphy.**

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.

Surveillance

'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

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

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.

5. THE AUTHORISATION PROCEDURE

Before undertaking a surveillance activity, written authorisation from the appropriate Authorising Officer must be obtained.

Exceptionally an urgent oral authorisation may be necessary.

Authorisation in urgent cases

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.

An authorisation will not be urgent where the need for authorisation has been neglected or is of the officer's own making.

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

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.

Cancelling an authorisation

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.

No authorisation can be left to expire. All authorisations 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 must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by Wiltshire Council relating to the handling, storage and destruction of material obtained.

6. THE ROLE OF THE AUTHORISING OFFICER

Considering and granting authorisations

Authorising Officers are responsible for receiving, considering and, where appropriate, granting applications for authorisation. Authorising Officers should follow the steps set out in section 8 below when considering applications for authorisation.

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 the applicant must be informed.

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.

An Authorising Officer cannot delegate their power to authorise surveillance under RIPA to anyone else.

Urgent authorisations

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.

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.

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.

All urgent authorisations must be recorded immediately on the central register together with the date and time of the authorisation.

Duration

An Authorising Officer can grant a standard written authorisation for directed surveillance for any time period up to three months.

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

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 a high level of collateral intrusion is likely (i.e. relating to other people who are not targets but who may be affected by the operation) or provides access to confidential information.

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.

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 and must comply with data protection requirements and Wiltshire Council's codes of practice.

The results of all reviews must be recorded in the central record of authorisation.

Granting a renewal

Renewal applications should be made by the Officer who applied for the initial authorisation.

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.

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

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.

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.

7. APPLICATIONS FOR AUTHORISATIONS

Applications for authorisation to undertake directed surveillance must be made on form 1A and sent to the relevant departmental Authorising Officer listed in Appendix 2.

Standard application forms are held by the Legal Unit and can be obtained from the Intranet.

Review

Reviews of authorisations for directed surveillance must be completed on form 1B.

Renewal

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.

An application for renewal of an authorisation for directed surveillance must be made on form 1C.

The renewal application must be made to the Authorising Officer who granted the initial authorisation.

Cancellation

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.

Application for cancellation of the authorisation must be made on form 1D.

All cancellation decisions made by an Authorising Officer with regard to directed covert surveillance must also be recorded on form 1D.

8. CONSIDERING APPLICATIONS FOR DIRECTED SURVEILLANCE

This part of the policy lists the factors which Authorising Officers should consider upon receiving an application for an authorisation for directed surveillance.

Step 1: Is authorisation needed for this activity?

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 directed surveillance.

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.

At no time can an Authorising Officer authorise any intrusive surveillance.

Step 2: Is the activity necessary?

An Authorising Officer 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 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.

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 3: Is it proportionate?

If the activity is necessary, the Authorising Officer 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.

An Authorising Officer should first consider the following primary factors in determining whether the activity for which authorisation is sought is proportionate:

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 a Corporate Director or his deputy, as listed in Appendix 2.

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.

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 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.**

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.

9. 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.

10. 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 Authorising Officers 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 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 Senior Respoonsible 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:

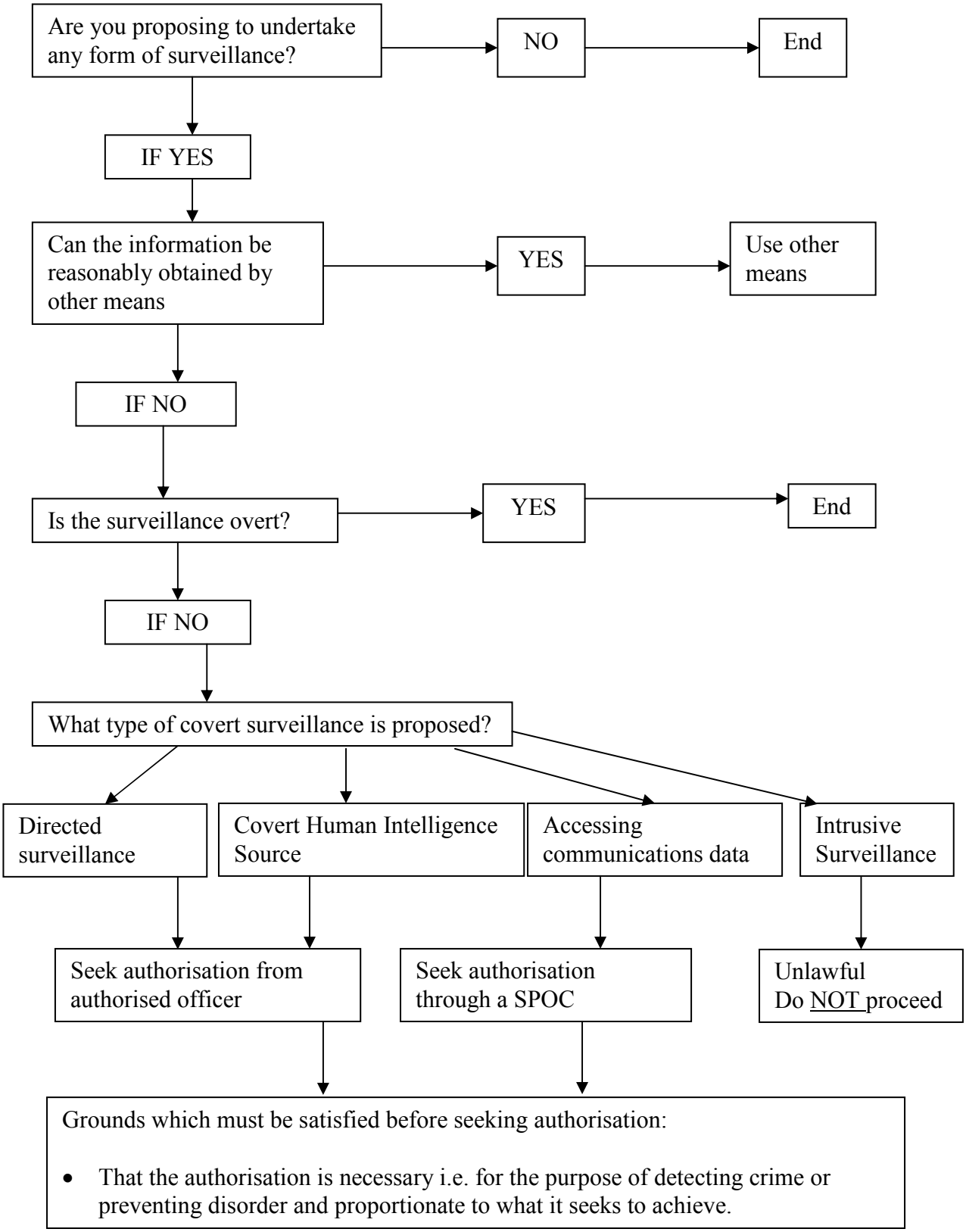
- The type of authorisation;
- The date on which the authorisation was given;
- Name/rank of the Authorising Officer;
- The unique reference number (URN) of the investigation/operation. This will be issued by the Legal Unit when a new application is entered in the Central Record. The applicant will be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

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.

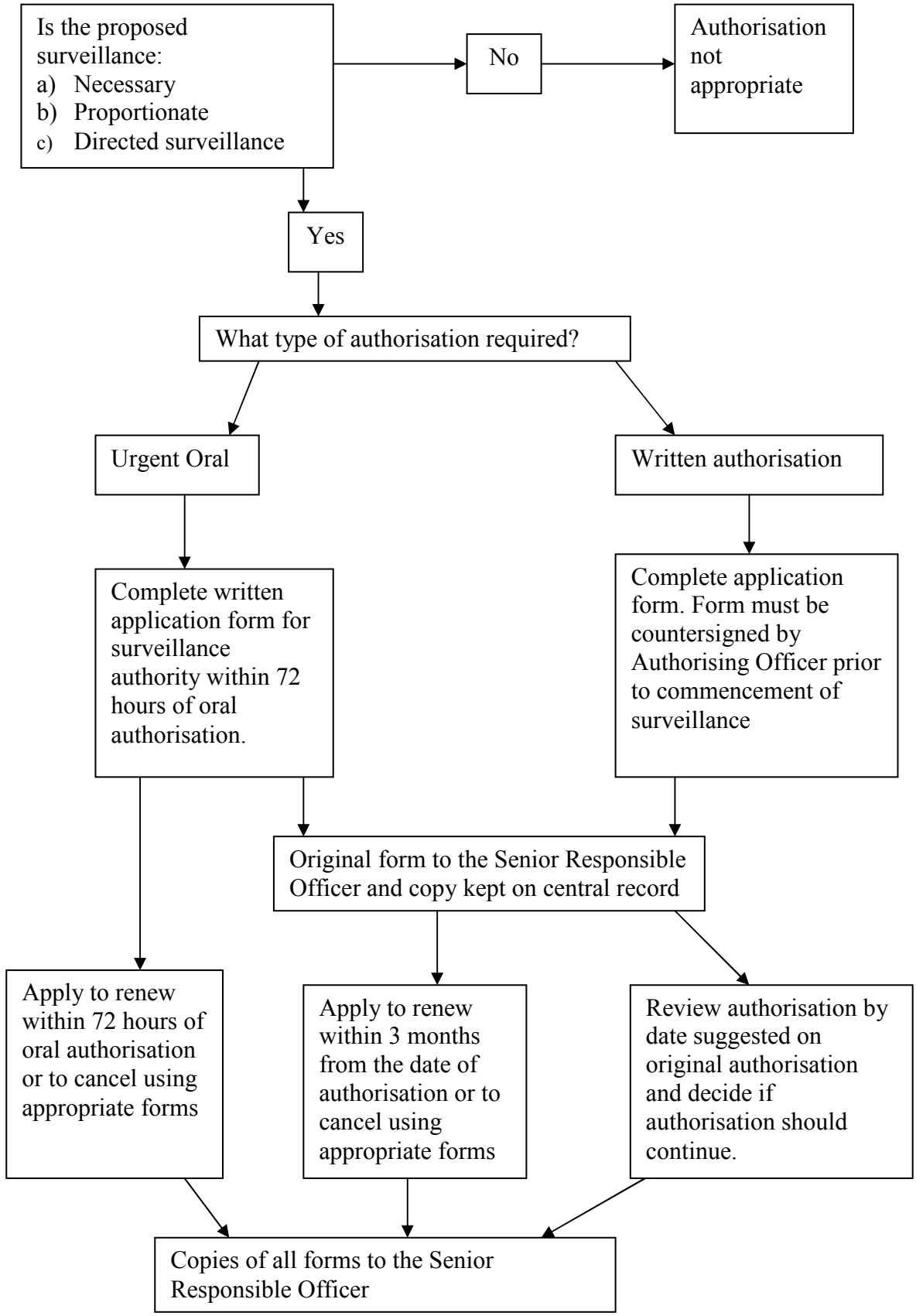
APPENDIX 1A

Do you need a RIPA authorisation?



APPENDIX 1B

RIPA Authorisation Process for Directed Surveillance



APPENDIX 2

List of Authorising Officers

1. <u>For standard or urgent oral authorisations:</u>

Where it is not likely that confidential information will be acquired

- Mike Wilmott, Development Manager, Browfort
- Derek Streek, Head of Housing Management, Salisbury
- Mandy Bradley, Service Director – Public Protection, County Hall
- John Carter, Head of Public Protection (Food and Environment), Bradley Road
- Steve Clover, Head of Commercial and Consumer Protection, Monkton Park
- Julie Higginbotham, Benefits Manager, Monkton Park

2. <u>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</u>

- Any Corporate Director

In their 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 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