OADBY & WIGSTON BOROUGH COUNCIL

POLICY AND PROCEDURES DOCUMENT

ON

DIRECTED SURVEILLANCE

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

Committee approval	Policy Finance and Development Committee 26 March 2019
Author	DM Gill
EIA	
Policy Version Number	2
Date of Policy Review	March 2020

INDEX PAGE NO.

APPENDICES

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 and will protect the Council from challenges to both the gathering of, and the subsequent use of, covertly obtained information enabling it to show that it has acted lawfully.

Non- compliance may result in:

(a) evidence being disallowed by the courts;

(b) a complaint to the Investigatory Powers Tribunal;

(c) a complaint of maladministration to the Ombudsman; or

(d0) 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 (August 2018) or any code of practice issued in replacement of this code of practice.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

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 arising from crime, meets the Directed Surveillance Crime Threshold and the Authorising Officer considers that covert surveillance is a proportionate way for the Council to obtain the desired information.

Any authorisation granted by the Authorising Officer must then be approved by a Justice of the Peace (JP) before it can be implemented. This process is set out at Section 10.

Section 11 of this policy covers the arrangements for working with or through other agencies for surveillance purposes.

Section 12 of this policy sets out the requirements for records management. This includes both departmental records and the central record which is maintained by the RIPA Co-ordinating Officer.

All officers considering seeking a RIPA authorisation **must seek advice** from the Head of Law and Governance at the earliest opportunity and in any event before an application is submitted for authorisation.

3. OVERSIGHT OF THE POLICY

The Senior Responsible Officer is responsible for the integrity of the process within Oadby and Wigston Borough 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 Investigatory Powers Commissioner's Office. 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 RIPA Co-ordinating Officer is responsible for the day to day oversight of applications and for the maintenance of the central record. The RIPA Co-ordinating Officer shall report to the Senior Responsible Officer any failings, training needs or improvements to the system.

Policy, Finance and Development Committee are responsible for ensuring that RIPA is being used consistently with this policy and that the policy remains fit for purpose. The Senior Responsible Officer will provide a report on Oadby and Wigston Borough Council's use of RIPA to the Policy, Finance and Development Committee 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 Policy, Finance and Development Committee for approval.

For the avoidance of doubt the Policy, Finance and Development Committee 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.

The Policy, Finance and Development Committee

This is the body defined in the Council's Constitution at Part 3 - Responsibility for Functions -

Committee Structure.

Code of Practice

Home Office Covert Surveillance and Property Interference Revised Code of Practice (August 2018) 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 the directly intended subjects of the investigation or operation.

Confidential Information

Confidential information consists of matters subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, 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.

Directed Surveillance crime threshold

The crime threshold applies only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of Communications Data.

Local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences or disorder associated with criminal that are either:

- punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months' imprisonment; or,

- relate to the underage sale of alcohol and tobacco.

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.**

Online Covert Activity

This is when internet is used to gather information from social media platforms and networks, such as Facebook and Twitter, during an operation. Depending on the level and frequency of viewings this may amount to directed surveillance as a result of the enthusiastic but misguided use of social media in pursuing allegations or seeking intelligence.

Where officers use social media networks they must have regard to the Home Office guidance set out below which advises that where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, consideration should be given for the need of an authorisation at the outset of the investigation and that:

- Officers must not create a false identity in order to 'befriend' or follow individuals on social networks without an authorisation under RIPA.
- Officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation
- The general rule of thumb is that the researching of open source material generally would not require an authorisation, however the repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, will require an authorisation and must only take place once a RIPA authorisation has been granted and approved by a Magistrate
- Officers should not ask family, friends, colleagues or any other third party to gain access on their behalf or otherwise use the Social Media Accounts of such people to gain access
- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites, a CHIS authorisation should be considered.

Judicial Approval

Local authority authorisations and notices under RIPA can only be given effect once an order approving the authorisation or notice has been granted by a JP.

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.

Property Interference and Incidental Property Interference

Entry on, or interference with, property or with wireless telegraphy are only available to the Police and Intelligence services. They are not something that the Council can authorise.

However, it may be that an act of property interference (for example, trespass when deploying covert camera equipment) has to be considered when undertaking authorised Directed Surveillance. RIPA provides that a Public Authority shall not be subject to any civil liability in respect of any such conduct which is incidental to correctly authorised directed surveillance activity and for which an authorisation is not available

In such circumstances the Head of Law and Governance should be contacted to advise on Corporate risk and liability.

RIPA Co-ordinating Officer (RCO)

The Head of Law and Governance is the RCO and is responsible for the day to day oversight of applications, the maintenance of the Register and the reporting to the Senior Responsible Officer of any failings, training needs or improvements to the system.

Senior Responsible Officer

The Head of Paid Service (Chief Executive)

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 AND APPROVAL PROCEDURE

Before undertaking a surveillance activity, written authorisation from the appropriate Authorising Officer must be obtained along with Judicial approval of the authorisation.

Exceptionally out of hours Judicial approval may be necessary.

If the authorisation is urgent and cannot wait to be handled the next working day then it may be necessary to:

- Make arrangements with the relevant HMCTS out of hour's legal staff. You will be asked about the basic facts and urgency of the authorisation.
- If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
- If urgency is agreed, then arrangements will be made for a suitable Justice of The Peace to consider the application. You will be told where to attend and give evidence.
- Attend the hearing as directed with two copies of both the counter-signed RIPA authorisation form or notice and the accompanying judicial application/order form.
- If the application is approved the Officer should provide the court with a copy of the signed judicial application/order form the next working day.

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 and judicial approval of the renewal should be sought 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. If, during the currency of an authorisation, the Authorising Officer is satisfied that the authorisation is no longer necessary, he must cancel it. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required.

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 Oadby and Wigston Borough 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 the SPOC listed in Appendix 3 and the applicant must be informed.

An Authorising Officer is empowered 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.

Duration

An Authorising Officer will grant a standard written authorisation for directed surveillance for three months. The period will take effect from the date of Judicial approval. Those conducting surveillance have a statutory obligation to cancel the authorisation as soon as the need for it no longer exists (see "cancelling an authorisation" in section 5 post).

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 with a minimum requirement that such reviews take place on a monthly basis. 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 Oadby and Wigston Borough 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 and that the Crime threshold is still being met. The authorisation for renewal must then be approved by a JP for it to take effect.

An authorisation may be renewed and approved 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

When completing an application for a warrant or authorisation, the case for authorisation must be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

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

Official standard application forms can be obtained from:

https://www.gov.uk/government/collections/ripa-forms--2

Review

Reviews of authorisations for directed surveillance must be completed on the standard form also available from the above web-site.

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, leaving sufficient time for the authorisation for renewal to be approved by a JP (see section 9 of this policy).

An application for renewal of an authorisation for directed surveillance must be made on the standard form also available from the above web-site.

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. If, during the currency of an authorisation, the Authorising Officer is satisfied that the authorisation is no longer necessary, he must cancel it. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required.

An application for cancellation of an authorisation must be made on the standard form also available from the above web-site.

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

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: Does the offence being investigated meet the 'Directed surveillance crime threshold?

An Authorising Officer must be satisfied that the crime or offence that is being investigated meets the Crime threshold. The crime or offence must be one that:

- attracts a maximum custodial sentence of six months or more; or,
- relates to the underage sale of tobacco and alcohol

If the crime or offence being investigated does not meet the threshold then an application for an authorisation for directed surveillance should not be made.

Step 2: Is authorisation needed for this activity?

An Authorising Officer must 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 3: Is the activity necessary and if so, why?

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.

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, other overt means having been considered and discounted.

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 arising from crime.

Step 4: Is it proportionate?

If the activity is necessary, the Authorising Officer must also believe that the activity is proportionate. In deciding whether the proposed surveillance is proportionate they should consider:

(i) Is the proposed covert surveillance proportional to the mischief under investigation?

(ii) Is it proportionate to the degree of anticipated intrusion on the target and others?

(iii) Is it the only option, other overt means having been considered and discounted?

Such considerations involve balancing the intrusiveness of the activity on the target and others, 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.

The following should therefore 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 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.**

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, communications between a Member of Parliament and another person on constituency matters, 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 (Chief Executive).

Risk of Collateral Intrusion

The Authorising Officer should take into account the risk of obtaining private information about persons who are not subjects of the investigation (collateral intrusion) before authorising applications for directed surveillance. The officer requesting authorisation should describe the activity in sufficient detail to include not only named individuals but also any others who may be at risk of collateral intrusion.

Wherever practicable, measures should be taken to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion cannot be avoided, the activities may still be authorised as long as the intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

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.

It is therefore imperative that all applications include a risk assessment in respect of the likelihood of collateral intrusion and details of any measures taken to limit it. This will enable the Authorising Officer to consider fully the proportionality of the proposed actions.

To comply with the ruling in the case of *R v Sutherland,* the Authorising Officer must also fully understand the capabilities and sensitivity levels of technical equipment intended to be used, and where and how it is to be deployed. The Authorising Officer should clearly set out what activity and what surveillance equipment is authorised in order that those conducting the surveillance are clear on what has been sanctioned.

9. THE ROLE OF THE JUSTICE OF THE PEACE

Approval of initial authorisations

Where an Authorising Officer has considered and authorised an application to use directed surveillance, that authorisation must be approved by a JP before the authorisation can take effect.

Applications to the JP should be made following the procedure in section 10 of this policy.

Where an authorisation is approved by the JP that authorisation takes effect from date on which the JP granted his or her approval.

Renewals

Where an Authorising Officer has considered and authorised the renewal of an existing authorisation to use directed surveillance, that renewal must also be approved by a JP before the initial authorisation expires. The renewal will then take effect on the date the initial authorisation expires.

Cancellations and reviews

The JP does not play a role in the cancellation or review of authorisations.

10. APPLICATIONS FOR APPROVAL BY THE JUSTICE OF THE PEACE

A link to the Home Office Guidance on the full Judicial Approval Process can be found at Appendix 4. The process is as follows:

Once the Authorising Officer has approved the application, the officer requesting authorisation should contact the Listings Office at Leicester Magistrates Court to arrange a hearing.

The Authorising Officer should where practicable attend the court along with the requesting officer. Once at court, the officers should provide the JP with a copy of the original RIPA authorisation form and any supporting documents setting out the case. This forms the basis of the application and should contain all the information the officers wish to rely upon.

The JP should ensure that sufficient privacy is given to the hearing commensurate with the covert nature of the investigation (i.e. no press, public, subject or legal representative present or court staff apart from Legal Adviser). The JP will consider the papers presented and will ask any additional questions of either officer in order to conclude whether an order to approve the grant of a RIPA authorisation should be made. It is for the papers to make the case and the JP cannot rely solely on oral evidence if this is not reflected or supported by the papers.
In deciding whether or not to approve the authorisation the JP must be satisfied that:

- there are reasonable grounds to believe that the authorisation is necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the JP is considering the matter

- that the application has been authorised by an Authorising Officer

The original RIPA authorisation should be shown to the JP if requested but will ultimately be retained by the RIPA co-ordinating Officer for the Council's records.

The officer attending the hearing should also provide the JP with an unsigned completed judicial application/order form

The order form section of this form will be completed by the JP and will be the official record of the JP's decision. This form should be retained and provided to the RIPA co-ordinating Officer for the Council's Central Record.

11. 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 and ensure that copies of the authorisation and judicial approval relied upon are obtained from the tasking authority.

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.

12. RECORDS MANAGEMENT

The Council must keep a detailed record of all authorisations, Judicial approvals, 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 RIPA Co-ordinating Officer.

All Authorising Officers must send all **original** applications for authorisation to the RIPA Co-ordinating Officer. Each document will be given a unique reference number, the original will be placed on the Central Record and a copy will be returned to the applicant.

Copies of all other forms used and the original Judicial approval form must be sent to the RIPA Co-ordinating 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, and any Judicial approval granted, to include the following:

- A copy of the application and a copy of the 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.

- A copy of the order approving or otherwise the grant or renewal of an authorisation from a JP.

Central Record Maintained by the RIPA Co-ordinating Officer

A central record of all authorisation forms, whether authorised or rejected, is kept by the RIPA Co-ordinating Officer. The central record must be readily available for inspection on request by the Investigatory Powers Commissioner's Office.

The central record must be updated whenever an authorisation is granted, reviewed, 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;

- Details of attendances at the Magistrates Court to include date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;

- The unique reference number (URN) of the investigation/operation. This will be issued by the Head of Law and Governance 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;

- 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;

- In the case of a self-authorisation by the Authorising Officer, a statement in writing that he/she expressly authorised the action
- If the authorisation was reviewed, when it was reviewed and who authorised the review, including the name and rank/grade of the Authorising Officer

- The date and time that the authorisation was cancelled.

It also contains a comments section enabling oversight remarks to be included for analytical purposes.

The appointment of the Head of Law and Governance as the RIPA Co-Ordinator ensures that there is an awareness of the investigations taking place. This would also serve to highlight any unauthorised covert surveillance being conducted.

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 Head of Law and Governance or the Senior Responsible Officer.

Complaints procedure

The council will maintain the standards set out in this guidance and the Codes of Practice (See Appendix D). The Investigatory Powers Commissioner's Office (IPCO) has responsibility for monitoring and reviewing the way the council exercises the powers and duties conferred by RIPA and where errors occur they shall be reported to the IPCO.

Contravention of the Data Protection Act 2018 and the General Data Protection Regulation may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of this guidance should be made using the council's own internal complaints procedure.

To request a complaints form, please contact the Monitoring Officer, Bushloe House, Station Road, Wigston Leicester, LE18 2RD.

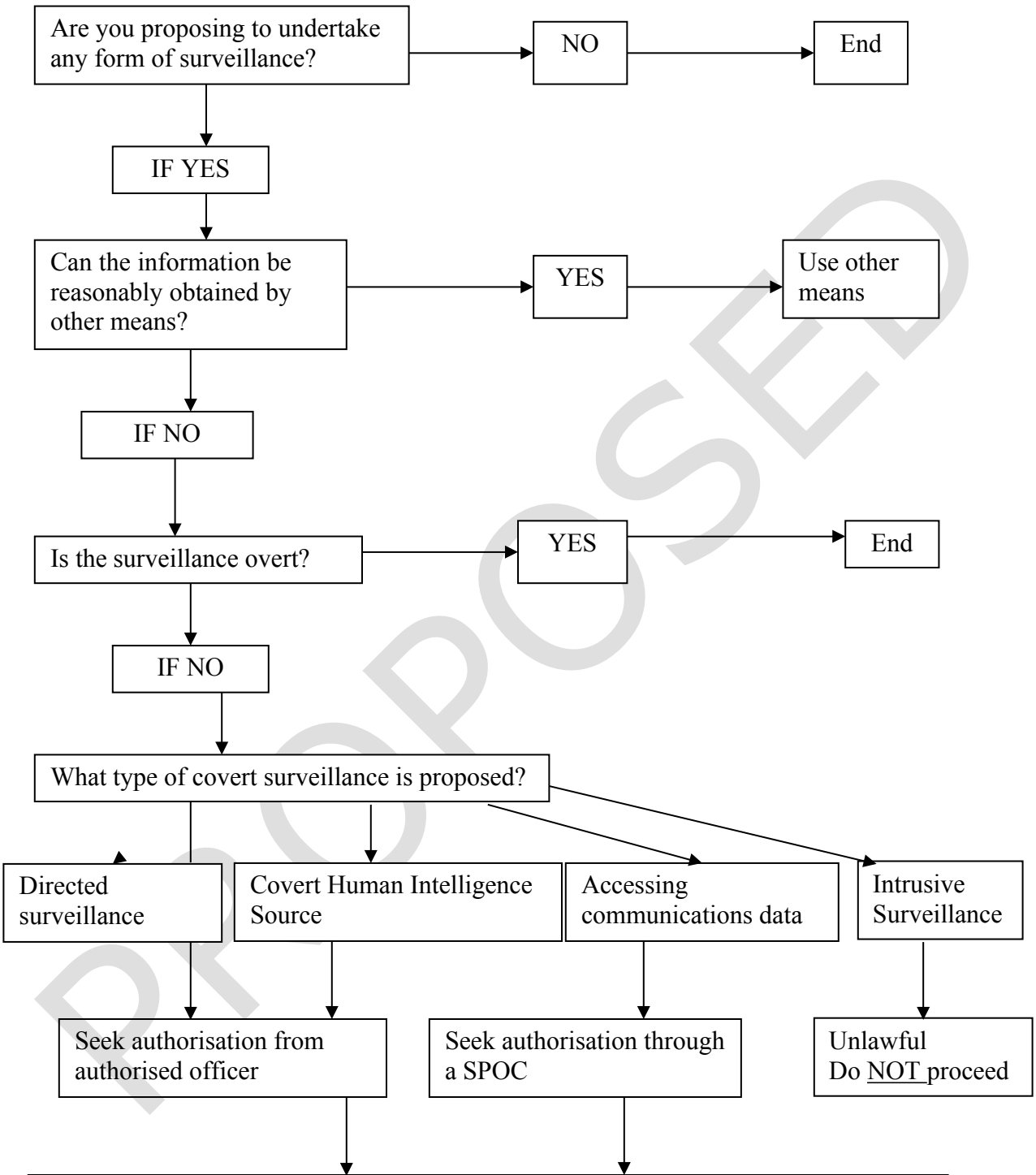
The 2000 Act also established an Independent Tribunal which investigates complaints about how RIPA is used. That Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the government. The Tribunal has full powers to investigate and decide any complaint within its jurisdiction.

Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal, PO BOX 33220, London SWLH 9ZQ
Telephone 020 7035 3711

APPENDIX 1A

Do you need a RIPA authorisation?

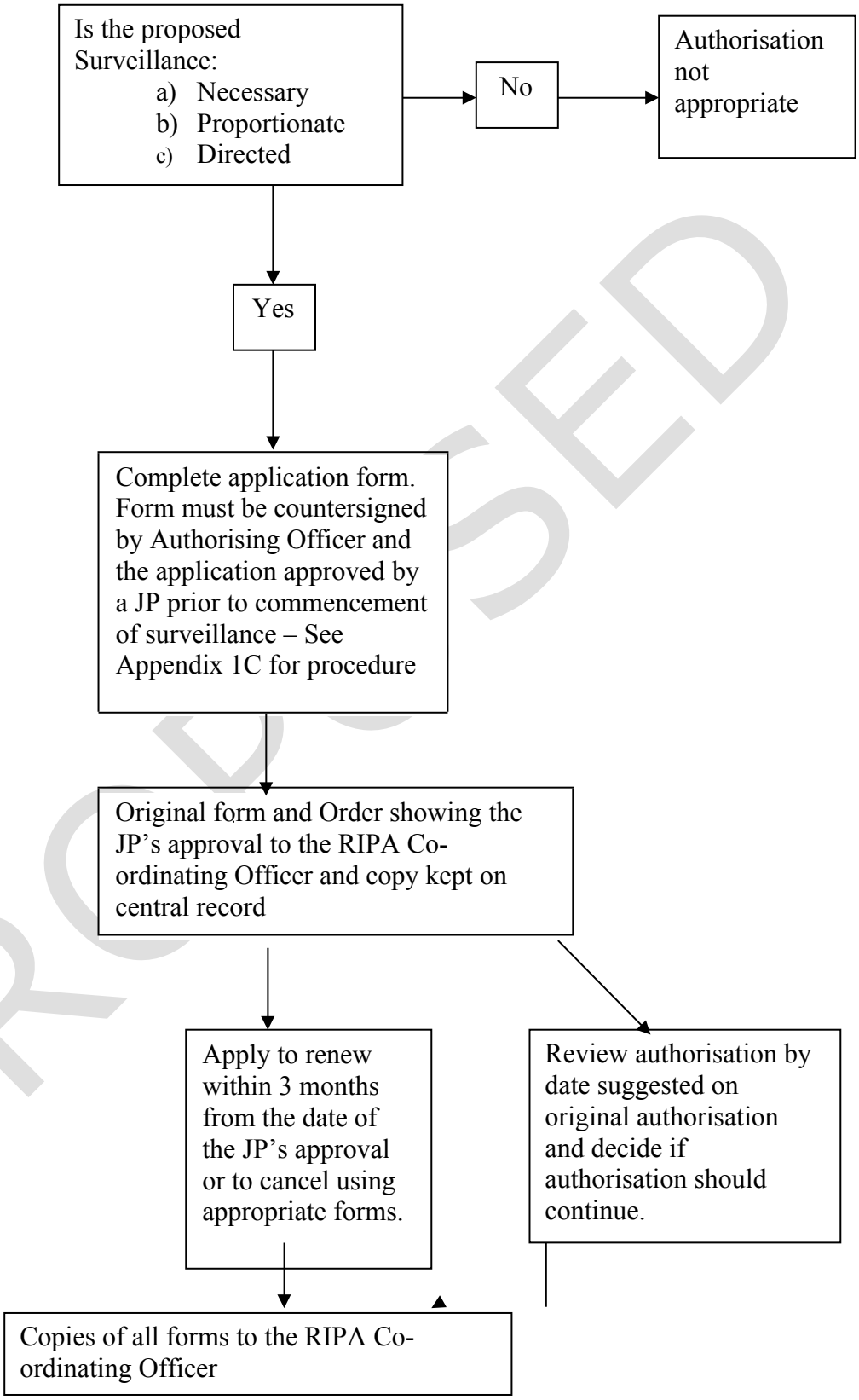


Grounds which must be satisfied before seeking authorisation:

- That the authorisation is necessary i.e. for the purpose of detecting crime or preventing disorder and proportionate to what it seeks to achieve.
- That, in the case of Directed Surveillance only, the crime or offence being investigated meets the Directed Surveillance Crime Threshold.

APPENDIX 1B

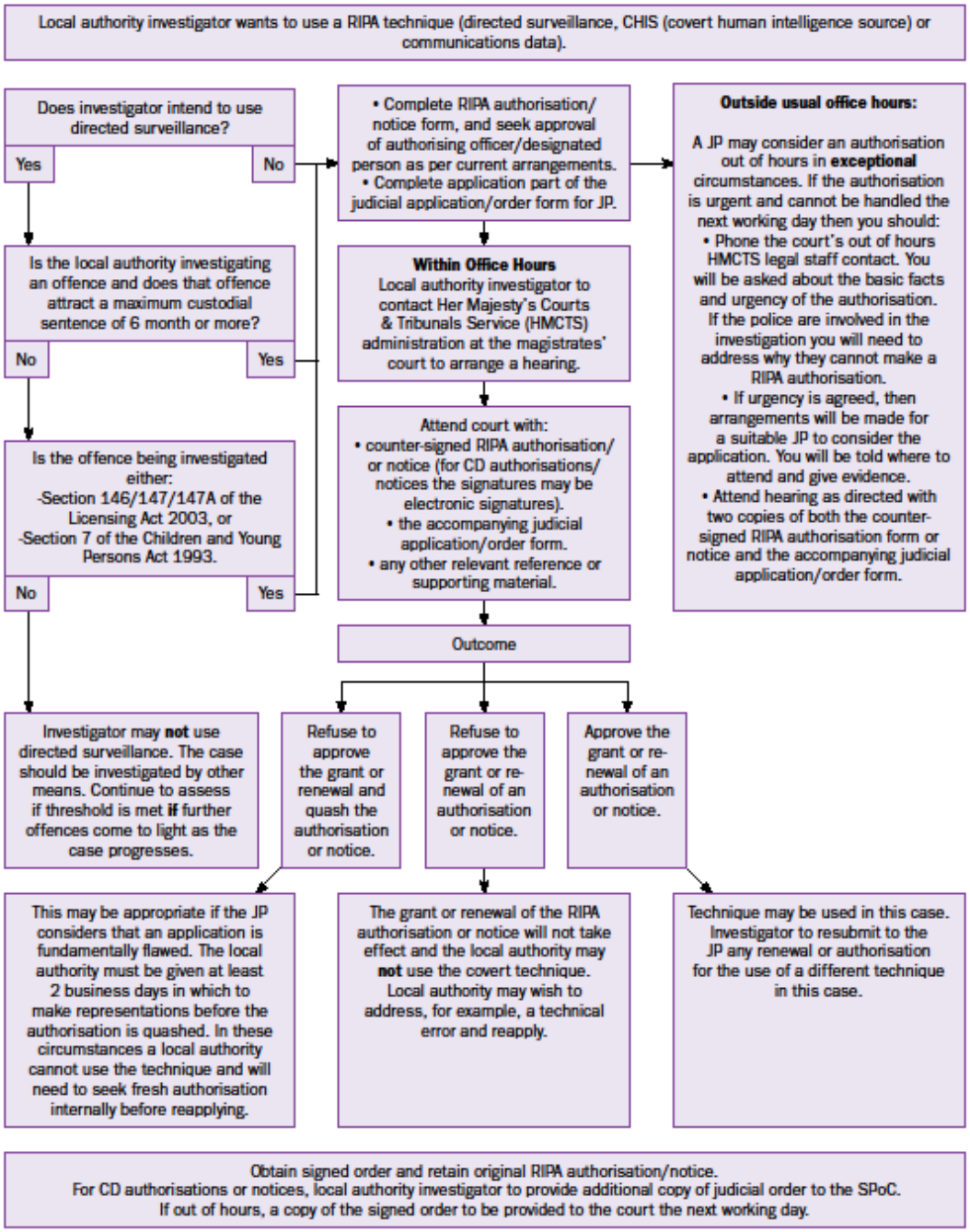
RIPA Authorisation and Approval Process for Directed Surveillance



APPENDIX 1C

ANNEX A - Extract from Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance.

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



APPENDIX 2

List of Authorising Officers

1. <u>For standard authorisations:</u>

Where it is not likely that confidential information will be acquired

- Chief Executive
- Director of Finance & Transformation
- Head of Law and Governance

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>

- The Head of Paid Service (Ch. Executive)

In their absence:

- The Director of Finance and Business Transformation

APPENDIX 3

List of Designated Persons

Designated Persons consider applications for access to communications data.

The Council's Designated Persons are as follows:

- Chief Executive
- Director of Finance & Transformation
- Head of Law and Governance

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 SPOC is as follows:

- The National Anti-Fraud Network

APPENDIX 4

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa