OADBY & WIGSTON BOROUGH COUNCIL

CORPORATE POLICY AND PROCEDURES DOCUMENT

ON

COVERT HUMAN INTELLIGENCE SOURCES

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

ADVISORY NOTE - IF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS) IS BEING CONSIDERED URGENT ADVICE SHOULD BE SOUGHT FROM THE HEAD OF LAW AND GOVERNANCE OR THE SENIOR RESPONSIBLE OFFICER (CHIEF EXECUTIVE) BEFORE ENGAGEMENT TAKES PLACE.

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 intelligence operations. 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

(d) 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 7 of this policy. Applications are made to Authorising Officers.

All Officers making applications and Authorising Officers should be aware of and familiar with the Home Office Covert Human Intelligence Sources 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/742042/20180802_CHIS_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 operational activity is necessary for the detection or prevention of crime or for preventing disorder where this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment, and the Authorising Officer considers that covert operational activity 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 before it can be implemented. This process is set out at Section 10.

Section 11 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.

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 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 Investigatory Powers Commissioner's Office, (IPCO). 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 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 Oadby and Wigston Borough Council's use of RIPA to 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 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 the use of a covert human intelligence source. Authorising Officers are listed at Appendix 2.

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 Human Intelligence Sources 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.

Covert Human Intelligence Sources (CHIS)

The conduct and use of a covert human intelligence source means in effect the use of an informant. In some cases this could include a test purchase or undercover Officer.

The conduct and use of a covert human intelligence source occurs when a person establishes or maintains a personal or other relationship with a person:

- for the covert purpose of using the relationship to obtain information or to provide access to any information to another person; or
- in order to disclose information covertly obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

A person may be a CHIS if they induce, ask or assist another person to engage in the conduct described above.

RIPA does <u>not</u> apply in circumstances where members of the public <u>volunteer</u> information to the Council or to contact numbers set up to receive information.

An authorisation will however be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the public authority.

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier for the purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter) although an Officer covertly watching a particular transaction may require an authorisation for directed surveillance.

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

NB Special safeguards apply to the use or conduct of vulnerable individuals or juveniles. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who may need protecting from exploitation. A vulnerable individual will only be authorised to act as a source in the most exceptional circumstances.

A juvenile is a young person under 18. Juveniles can be authorised as sources for four months. On no occasion can a child under 16 years of age be authorised to give information against his or her parents or anyone with parental responsibility for that child.

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 Justice of the Peace (JP).

RIPA Co-ordinating Officer (RCO)

The Head of Law and Governance is the RCO 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), Oadby and Wigston Borough Council

5. THE AUTHORISATION AND APPROVAL PROCEDURE

Before undertaking use of CHIS, 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 until 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. Where practicable the Authorising officer should also be in attendance at the hearing.

- 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.

Approval in emergency cases

In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it e.g. when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening.

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 operation must apply to have that authorisation cancelled when the investigation or operation for which authorisation was given has ended, the authorised operation activity has been completed, or the information sought is no longer necessary. If 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 operation is expected to continue beyond the duration of the authorisation, or cancelled, if

the operation 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 2 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 operation under RIPA to anyone else.

Duration

Written authorisation for a CHIS will cease to have effect at the end of a period of twelve months beginning with the day on which it took effect (which is the date of approval by a Justice of the Peace), unless it is renewed. Those conducting operations 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, ante).

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 operational activity. The Applicant must give sufficient information about the product of the operation 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 operation 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. The authorisation for renewal must then be approved by a Justice of the Peace 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.

Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled. The Authorising Officer should be satisfied that all welfare matters have been addressed.

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 operational activity.

7. APPLICATIONS FOR AUTHORISATIONS

Before deciding on this course of action, legal advice must be sought from the Head of Law and Governance.

All council Officers must receive authorisation in writing before undertaking the conduct and use of a CHIS.

Applications for authorisation to use a CHIS must be made on the official form sent to one of the Authorising Officer listed in Appendix 2.

Official forms are available from: https://www.gov.uk/government/collections/ripa-forms--2

For both vulnerable individuals and juveniles only the Head of Paid Service can give authorisation.

Duration

Written authorisation for a CHIS will cease to have effect at the end of a period of twelve months beginning with the day on which it took effect (the date of approval by a Justice of the Peace), unless it is renewed.

Review

Reviews of authorisations for the conduct and use of a CHIS must be completed on the official form.

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 Justice of the Peace (see section 9 of this policy).

Applications for renewal of an authorisation for the conduct and use of a CHIS must be completed on an official form.

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

Cancellation

The Officer responsible for undertaking the authorised operation must apply to have that authorisation cancelled when the investigation or operation for which authorisation was given has ended, the authorised operation activity has been completed, or the information sought is no longer necessary. It is a statutory requirement that authorisations are cancelled as soon as they are no longer required.

An application for cancellation of an authorisation for the conduct and use of a CHIS must be made on an official form.

Cancellation decisions must be recorded on the same form by the Authorising Officer making the decision.

8. CONSIDERING APPLICATIONS FOR THE USE OF A CHIS

This part of the policy lists the factors which Authorising Officers should consider upon receiving an application for an authorisation for the use of a CHIS.

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 manipulation of a relationship to gain any information, regardless of whether or not there is an intention to acquire private information.

An Authorising Officer should interpret the definitions broadly when determining whether an activity is covert or if the use of a CHIS is likely to result in the manipulation of a relationship, with information being obtained. When in doubt, the authorisation procedure must always be followed.

Step 2: 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 or of preventing disorder associated with a 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 associated with a crime.

Step 3: Is it proportionate?

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

(i) Is the proposed activity 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;

- 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.

Provisions for the management of the source and records

When considering applications for the use of a CHIS, an Authorising Officer must take into account the provisions of section 29 of RIPA and the Source Records Regulations (2000 SI No. 2725) made under it before authorising the conduct or use of a CHIS.

Section 29(5) requires the Authorising Officer to be satisfied that arrangements are in place for the careful management of the source and that records are maintained relating to the source which contain the particulars specified in the Source Records Regulations.

The Authorising Officer must therefore**:**

(a) be satisfied that the conduct and/or use of the CHIS is both necessary and proportionate to what is sought to be achieved. This will be addressed by following the procedure provided in this section;

(b) be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. This must address health and safety issues through a risk assessment;

(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

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

Controller and Handler

When a CHIS is used, a 'Handler' (who can be an officer of the Council), and who must have received appropriate training, should be designated as having the day to day responsibility for dealing with the CHIS. This responsibility shall extend to security, safety and welfare of the CHIS. In addition, a 'Controller' should be designated to have the general oversight of the use made of the CHIS. These requirements also apply in cases in which the CHIS is an officer of the Council.

Vulnerable Individuals and Juveniles

Special safeguards apply to the use or conduct of vulnerable individuals or juveniles. When considering applications for the use of a CHIS, an Authorising Officer must identify whether the proposed CHIS is a vulnerable or juvenile individual. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who may need protecting from exploitation. A vulnerable individual will only be authorised to act as a source in the most exceptional circumstances.

A juvenile is a young person under 18. Juveniles can only be authorised as sources for one month. On no occasion can a child under 16 years of age be authorised to give information against his or her parents or anyone with parental responsibility for that child.

Before deciding on this course of action, legal advice must be sought from the Head of Law and Governance.

Where the proposed activity involves the use of a vulnerable person or juvenile as a CHIS, only the Head of Paid Service can give authorisation.

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 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. THE ROLE OF THE JUSTICE OF THE PEACE

Approval of initial authorisations

Where an Authorising Officer has considered and authorised an application to use a CHIS, that authorisation must be approved by a Justice of the Peace before the authorisation can take effect.

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

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

Renewals

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

Cancellations and reviews

The Justice of the Peace 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 3. 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 Justice of the Peace must be satisfied that:

- there were reasonable grounds for the local authority to believe that the authorisation was necessary and proportionate and there remain reasonable grounds for believing that these requirements are satisfied at the time when the Justice of the Peace is considering the matter

- that there were reasonable grounds for the local authority to believe that arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA and there remains reasonable grounds for believing that these requirements are satisfied at the time when the Justice of the Peace is considering the matter

- that there were reasonable grounds for the local authority to believe that the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended) were satisfied and there remain reasonable grounds for believing that these requirements are satisfied at the time when the Justice of the Peace is considering the matter

- that the local authority application has been authorised by an Authorising Officer

- the grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections for RIPA:

  -29(7)(a) (for CHIS)

  -30(3) (for CHIS and Directed Operation)

- any other conditions that may be provided for by an order made by the Secretary of State were satisfied.

The original RIPA authorisation should be shown to the JP if requested but ultimately will 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. RECORDS MANAGEMENT

The Council must keep a detailed record of all authorisations, Judicial application/order forms, 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 Judicial application/order forms 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 approvals 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 operation has taken place;
- The frequency of reviews prescribed by the Authorising Officer;
- A record of the result of each review;
- In the case of a self-authorisation by the Authorising Officer, a statement in writing that he/she expressly authorised the action
- 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 Justice of the Peace.

The profile containing the true identity of the CHIS should be confidentially stored, separately from other CHIS records.

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.

The central record must be updated whenever an authorisation is granted, renewed, reviewed or cancelled. These records should be retained for a period of at least five years from the ending of the authorisations to which they relate. Where used as evidence, 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 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;
- 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 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;
- 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.

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 operation. 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.

Complaints procedure

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.

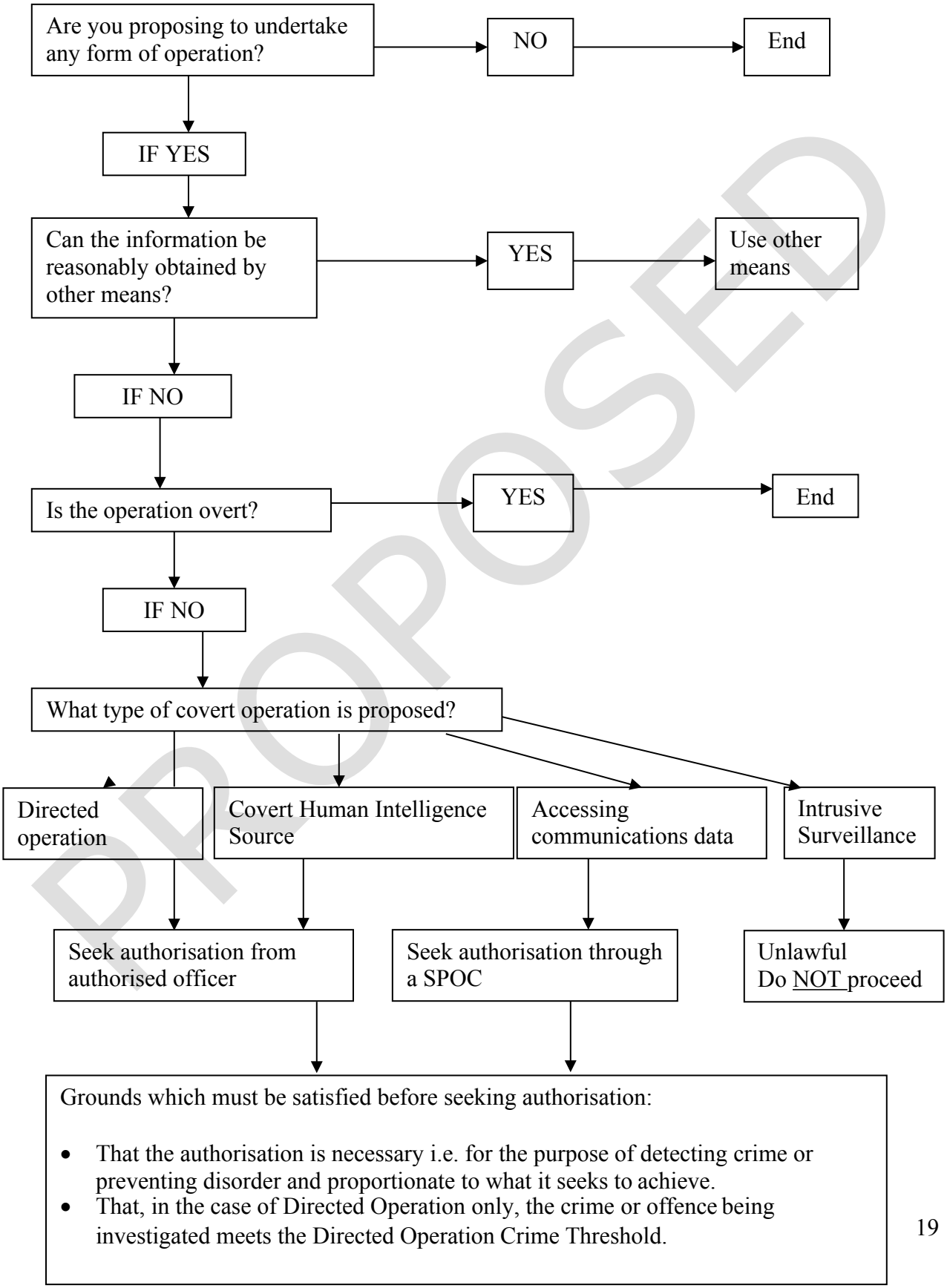
The 2000 Act also established an Independent Tribunal which investigates complaints about how RIPA is used. That Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the government. The Tribunal has full powers to investigate and decide any complaint within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

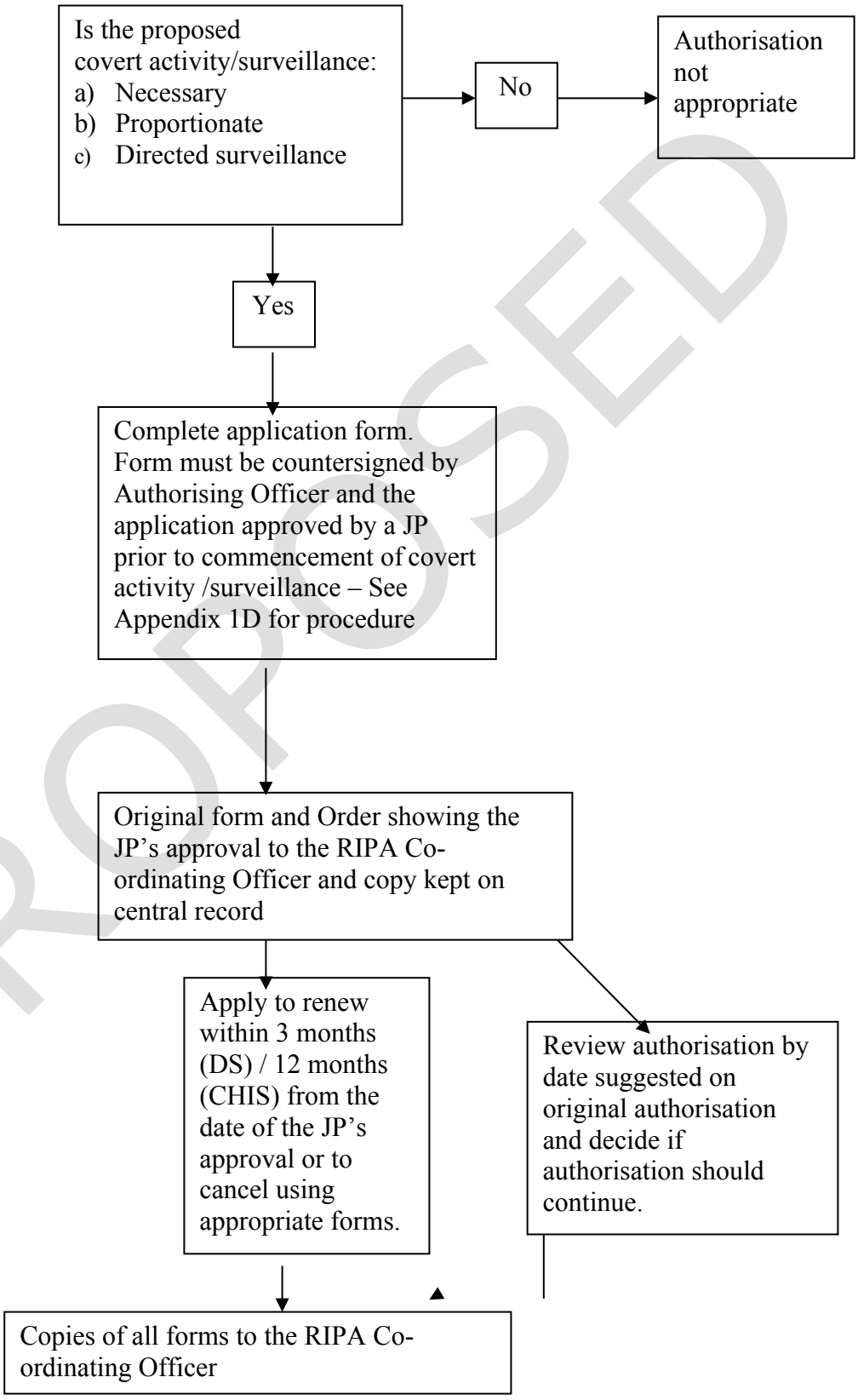
APPENDIX 1A

Do you need a RIPA authorisation?



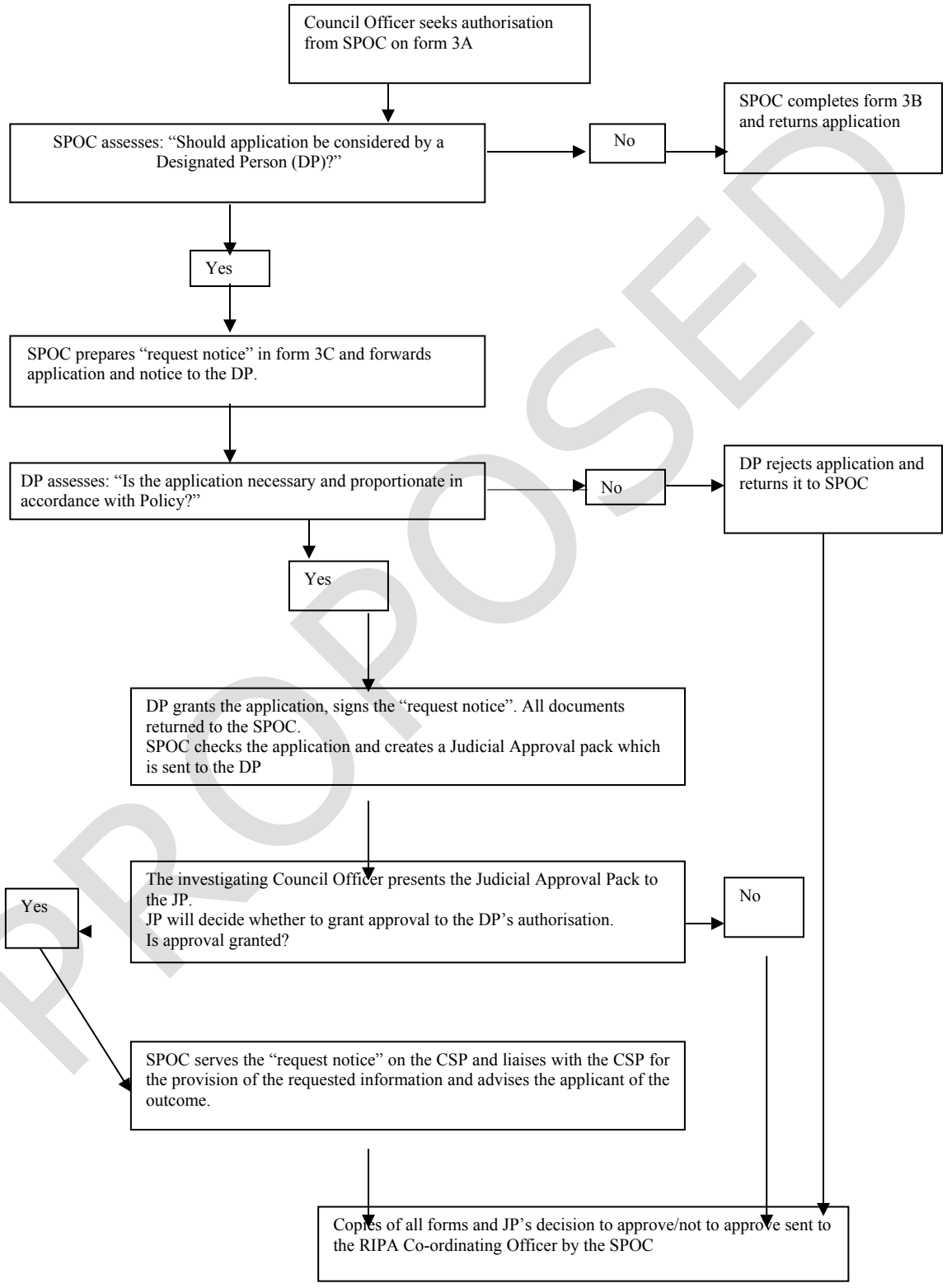
APPENDIX 1B

RIPA Authorisation and Approval Process for Directed Operation and CHIS



APPENDIX 1C

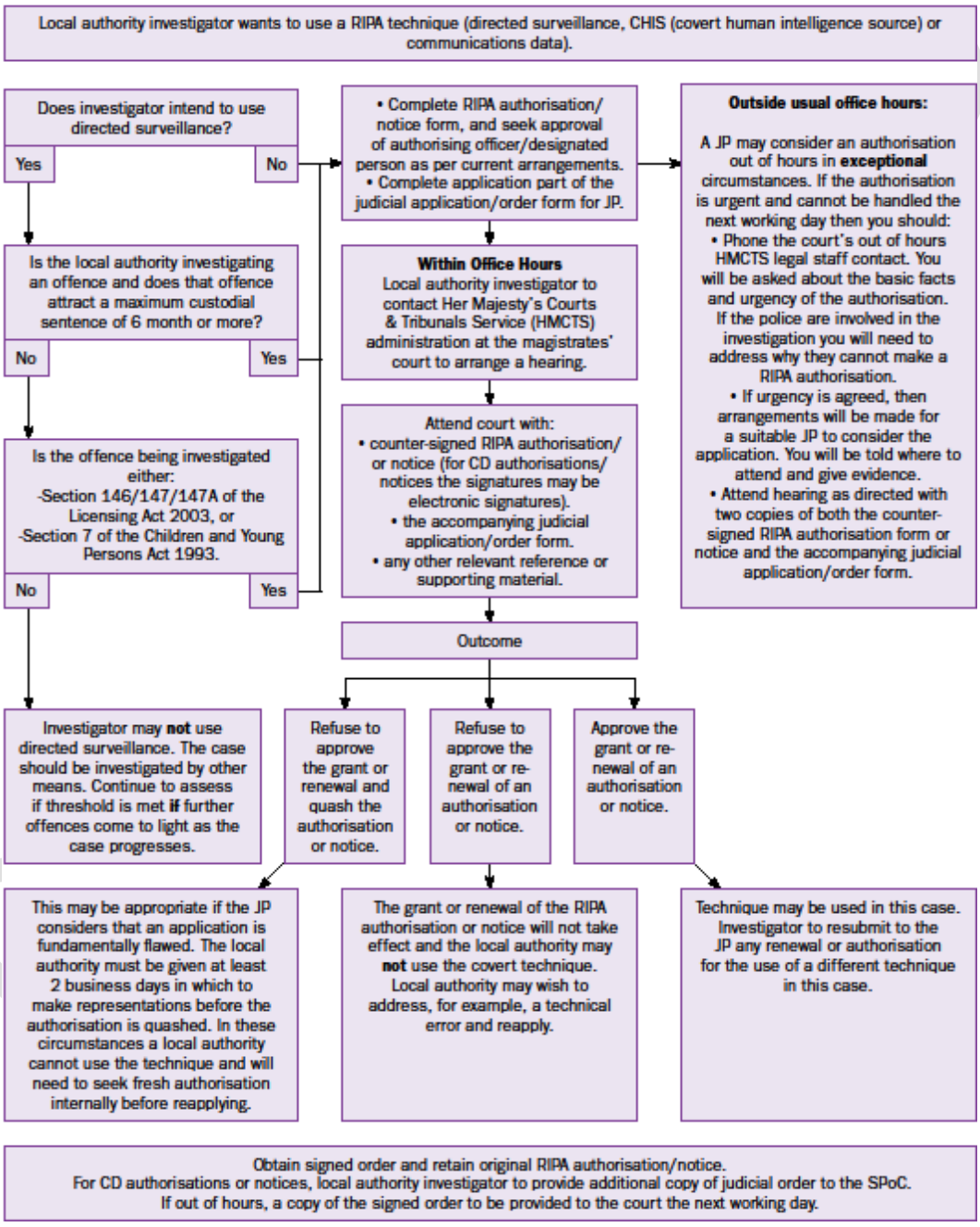
Application Process for Authorisation and Approval to Access Communications Data



APPENDIX 1D

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. For standard authorisations:

Where it is not likely that confidential information will be acquired

- The Head of Paid Service
- The Director of Finance and Business Transformation
- The Head of Law and Governance

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

- The Head of Paid Service

In their absence:

- The Director of Finance and Business Transformation

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 3

Home Office Guidance on Local Authorities use of RIPA

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

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