**REGULATION OF INVESTIGATORY POWERS ACT 2000**

**POLICY AND PROCEDURAL GUIDE[1]**

| | |
|---|---|
| Adopted by Council: | 26/9/19 |
| Reviewed/amended[2] | 16/11/22-to amend names of Relevant officers only |
| Reviewed/amended | 15/04/2024 |
| Reviewed/amended | 30/12/2024 |

# INDEX

## 1. INTRODUCTION

1.1 This policy document shall be readily available at the offices of Newark and Sherwood District Council ("the Council). It will be available on the Intranet for staff use only and the Internet site of the Council for public to view.

1.2 The purpose of this document is to ensure that the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA) and any associated codes of practice or Government (or other) guidance and as maybe amended from time to time.

1.3 This document provides guidance on the regulation of any covert surveillance that is carried out by Council officers. This includes the use of undercover officers, informants and private investigators and other agents of the Council.

1.4 Any covert surveillance will have to be authorised and conducted in accordance with RIPA, the statutory codes of practice and this Guide. Any such covert surveillance shall only be for one of the purposes set out in this Guide and for a purpose which the Council is legally required or empowered to investigate as part of its functions.

1.5 Covert surveillance will only be used by the Council where it is satisfied that such use to be proportionate to the seriousness of the crime or matter being investigated, and the history and character of the individual(s) concerned.

1.6 Before requesting authorisation, Investigating Officers will have regard to this document and the statutory Codes of Practice issued under section 71 of RIPA. The

Codes of Practice are available from the RIPA co-ordinator and direct from the Home Office at http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

1.7 Authorising officers will have to consider whether it is reasonable, necessary and proportionate for Investigating Officers to undertake covert surveillance and whether it is possible to obtain the evidence through other means.

1.8 Authorising Officers must give detailed consideration to the risk of collateral intrusion, i.e. the risk of intruding into the privacy of others while watching someone else. All reasonable and practical steps will have to be taken to minimise or negate this risk.

1.9 There should be no situation where an officer engages in covert surveillance without obtaining authorisation in accordance with the procedures set out in this document, the statutory Codes of Practice and from RIPA.

1.10 Any queries concerning the content of the document should be addressed to the RIPA co-ordinator. Details of all relevant co-ordinator and authorising officer details are on page 18 of this document.

1.11 If you are in any doubt as to whether RIPA applies to any activity you intend to carry out, please seek legal advice from the team or RIPA co-ordinator before you undertake the activity.

1.12 This policy should be read in conjunction with the Council's social media policy for employees and the Social Media Policy in respect of Investigations.

## 2. THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

### 2.1 The background to RIPA

RIPA provides a legal framework for the control and regulation of surveillance and information gathering techniques which public authorities undertake as part of their duties. On the 25 September 2000 the Regulation of Investigatory Powers Act 2000 was brought into force in England and Wales. The need for such control arose as a result of the Human Rights Act 1998. Article 8 of the European Convention on Human Rights states that:-

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

This right under Article 8 is a "qualified right" and public authorities can interfere with this right for the reasons given in paragraph 2 of Article 8 (above).

RIPA provides the legal framework for lawful interference.

### 2.2 The scope of this Policy and Guide

This Guide intends to cover the surveillance and information gathering techniques which are most likely to be carried out by the Council.

Neither RIPA nor this Guide covers the use of any "overt" surveillance (i.e. out in the open so that the person/people being observed would know), general observation that forms part of the normal day to day duties of officers, the use of equipment to merely reinforce normal sensory perception (i.e. binoculars) or circumstances where members of the public who volunteer information to the Council.[3]

RIPA does not normally cover the use of overt CCTV surveillance systems since members of the public are aware that such systems are in place.

If an Investigating Officer envisages using any CCTV system for surveillance they should contact the RIPA co-ordinator.

RIPA deals with a wide variety of surveillance types. Some of the other techniques that are covered by RIPA will not, or cannot, be used by local authorities. These include:-

1. Interception of any communication such as postal, telephone or electronic communications without both the sender and receiver's permission; ie to prevent the addressee receiving the communication or reading it prior to them receiving it.

2. The acquisition and disclosure of information as to who has sent or received any postal, telephone or electronic communication; and

3. The covert use of surveillance equipment within any premises or vehicle, including business premises and vehicles with the intention of covertly gathering information about the occupant(s) of such premises or vehicles.

## 2.3 Consequences of not following RIPA

Section 27 of RIPA provides that surveillance shall be lawful for all purposes if authorised and conducted in accordance with an authorisation granted under RIPA.

Lawful surveillance is exempted from civil liability.

Although not obtaining authorisation does not make the authorisation unlawful per se, it does have serious consequences:-

(i) Evidence that is gathered may be inadmissible in court;

(ii) The subjects of surveillance can bring their own proceedings or defeat proceedings brought by the Council against them on human rights grounds, ie. we have infringed their rights under Article 8;

(iii) If a challenge under Article 8 is successful the Council could face a claim for financial compensation;

(iv) A complaint could be made to The Investigatory Powers Commissioner's Office and

(v) Any person who believes that their rights have been breached can have their complaint dealt with by way of a tribunal.

All of the above have a financial impact on the Council as well as harming our reputation with the public, the courts and other professionals.

### 2.4 The Surveillance Commissioner

Investigatory Powers Commissioner's Office (IPCO) provides independent review and regulation of the use of investigatory powers by intelligence agencies, police forces, councils and other public authorities.

The IP Commissioner and his Judicial Commissioners are responsible for regulating and overseeing the use of investigatory powers by public authorities which include law enforcement, the intelligence agencies, prisons, local authorities and other government agencies (e.g. regulators). In total over 600 public authorities and institutions have investigatory powers.

The IPCO has unrestricted access to all locations, documentation and information systems as necessary to carry out their full functions and duties. They regularly review the way in which public authorities implement the requirements of RIPA. The Council will receive periodic visits from the IPCO. They will check to see if the Council is complying with RIPA.

It is important that the Council can show, with appropriate evidence, that it complies with this Policy and guidance and with the provisions of RIPA.

## 3. COVERT SURVEILLANCE

Covert surveillance means surveillance that is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is taking place.

There are three categories of covert surveillance:-

1. Directed surveillance (as defined by S26(6) of RIPA 2000)

2. Covert human intelligence sources (CHIS); and

3. Intrusive surveillance (but nothing in this Policy allows the authorising of "Intrusive surveillance" as defined in RIPA) ie. in respect of anything taking place on residential premises or in a private vehicle, involving the presence of an investigator on those premises/vehicles or carried out through a surveillance device such as a camera, recording device or similar.

### 3.1 Directed Surveillance (DS)

3.1.1 The majority of covert surveillance that will be undertaken by the Council will fall under the heading of Directed Surveillance (DS).

3.1.2 DS is defined as surveillance which is covert, but not intrusive, and is undertaken:-

(a) for the purpose of a specific investigation or operation;

(b) in such a manner as it is likely to result in obtaining private information about a person (whether or not that person is the target of the investigation or

operation); and

(c) in a planned manner and not by way of an immediate response whereby it would not be reasonably practicable to obtain an authorisation prior to the surveillance being carried out. i.e. if an officer walked past just as a fly-tip took place and recorded it on their mobile phone getting the drivers car registration and video of him.

3.1.3 It is irrelevant where the subject of the DS is being observed.

3.1.4 If you intend to instruct an agent (eg a process server or investigative service) to carry out the DS the agent must complete and sign the form marked "agent's agreement form" contained in **Appendix B**. The agent will be subject to RIPA in the same way as any employee of the Council would be. This is unlikely to happen often in the Council and advice must always be sought.

3.1.5 The flow chart in **Appendix C** gives guidance on when authorisation might be needed.

### 3.2 Covert Human Intelligence Sources (CHIS)

3.2.1 Under Part 2 RIPA 2000 Newark and Sherwood District Council is provided with lawful authority to obtain authorisation to use a covert human intelligence source to assist in the investigation of an operation to detect or prevent a crime or disorder. This involves the establishment or maintenance of a personal or other relationship with a person for the covert purpose of obtaining or disclosing private information. A CHIS is a person who:-

(a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

3.2.2 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. Eg using a false social media account to hide that you are from NSDC and engaging with someone on there.

3.2.3 A relationship is used covertly and information obtained is disclosed covertly, if and only if the relationship is used or the information is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question. Eg asking a pub landlord to listen in on a customer and report to NSDC about them; asking a neighbour to befriend someone suspected of ASB **and** to keep diary sheets about them for NSDC.

3.2.4 Covert Human Intelligence Sources may only be authorised if the following arrangements are in place:

- that there will at all times be an officer within the local authority who will have day to day responsibility for dealing with the CHIS on behalf of the authority, and for the CHIS's security and welfare;

- that there will at all times be another officer within the local authority who will have general oversight of the use made of the CHIS;

- that there will at all times be an officer within the local authority who has responsibility for maintaining a record of the use made of the CHIS; and

- that the records relating to the CHIS maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.

3.2.5 Legal advice should always be sought where any matters for investigation may involve the use of other enforcement agencies, including the police.

3.2.6 Special consideration must be given to the use of vulnerable individuals for CHIS. 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 is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

3.2.7 Any individual of this description, or a juvenile as defined below, should only be authorised to act as a CHIS in the most exceptional circumstances and only then when authorised by the Chief Executive or, in his absence, by the person acting as Chief Executive or in case of short term absences, by the Assistant Director Legal and Democratic Services and Monitoring Officer.

3.2.8 Before an Investigating Officer undertakes any surveillance involving a vulnerable individual they **must obtain legal advice** and consult the RIPA co-ordinator concerning any clarification on the administrative process. Also in these cases, any authorisation must be carried out by the Chief Executive or, in his absence, by the person acting as Chief Executive or in case of short term absences, by the Assistant Director Legal and Democratic Services and Monitoring Officer.

3.2.9 Special safeguards also apply to the use or conduct of juvenile CHIS; ie someone under the age of 18 years you wish to engage as a CHIS. On no occasion should the use or conduct of CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him.

3.2.10 There must be additional supervision and care taken for any proposed juvenile CHIS and the person responsible for their use must ensure that additional consideration of their wellbeing and safety is documented before, during and throughout the matter. Refer back to paragraphs 3.2.4 and 3.2.6 above

3.2.11 In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for juvenile sources should only be granted by the Chief Executive (or in his absence, the acting Chief Executive).

3.2.12 Before an Investigating Officer undertakes any surveillance involving a juvenile they must consult the RIPA co-ordinator.

3.2.13 The flow chart in **Appendix D** gives guidance on when authorisation might be needed.

**3.2.14 Any Investigating Officer considering the use of a CHIS must seek advice from the RIPA Co-ordinator before taking any steps in relation to a CHIS.**

### 3.3 Intrusive surveillance

3.3.1 Intrusive Surveillance is available only to the Police or other law enforcement agencies. Intrusive surveillance is defined as covert surveillance that:-

(a) is carried out in relation to anything taking place on/in any residential premises or in any private vehicle; and

(b) involves the presence of any individual on the premises or in the vehicle or is carried out by means of a surveillance device.

(c) if the device is not located on the premises or in the vehicle, it is not intrusive surveillance unless the device 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.

**Local authorities are not authorised to conduct intrusive surveillance.**

## 4. Procedure for Obtaining Authorisations

### 4.1 The Senior Responsible Officer (SRO):-

**Role:**

4.1.1 The Codes of Practice place certain responsibilities on the Senior Responsible Officer (RIPA Monitoring Officer).:- The Assistant Director Legal and Democratic Services and Monitoring Officer is designated the Council's Senior Responsible Officer (SRO). Code 3.22 states that "within every relevant public authority the SRO must be responsible for:-

(a) ensuring the integrity of the Council's RIPA processes.

(b) ensuring compliance with RIPA legislation and the Home Office Codes of Practice.

(c) engaging with the IPCO when its inspector conducts an inspection.

(d) overseeing the implementation of any post-inspection plans.

(e) ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations made by the IPCO inspection reports.

(f) ensuring that concerns are addressed, where IPCO inspection highlights concerns about the standards of Authorising Officers or application of RIPA.

4.1.2 To ensure these requirements are met the SRO maintains oversight and quality control in relation to RIPA functions and processes. The SRO maintains the Central Record of Authorisations and is also responsible for RIPA training and the heightening of awareness of RIPA issues throughout the Council and an oversight of all applications to ensure ongoing quality control.

**Authorising Officers:** **Appendix A** sets out the officers within the Council who can grant authorisations.

### 4.2 Role:

An Authorising Officer is an employee of Newark and Sherwood District Council who has received adequate training and has attained a level of competency to be able to provide authorisation. Authorising Officers can authorise, review and cancel directed surveillance. Each of them can authorise, review and cancel the employment of a juvenile or vulnerable CHIS, or the acquisition of confidential information.

4.2.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for local authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent. They must be distinct and in a senior role from the officer responsible for the conduct of an investigation.

4.2.2 A designated Authorising Officer must qualify **both** by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level and must maintain their training appropriately so as to have an understanding of the Act and the requirements that must be satisfied of before an authorisation can be granted.

4.2.3 Authorisations must be given in writing by the Authorising Officer.

4.2.4 Authorising Officers are also responsible for carrying out regular reviews of applications which they have authorised and also for the cancellation of authorisations.

### 4.3 Investigating Officers - What they must to before applying for authorisation.

4.3.1 An Investigating Officer is an officer within the Council who is involved in undertaking a specific investigation or operation. Investigating Officers should think about the need to undertake DS or CHIS before they seek authorisation. They need to consider whether they can obtain the information by using techniques other than covert surveillance. There is nothing that prevents an Investigating Officer discussing the issue of surveillance before progressing further. Consultation should take place with the Officer's manager and/or legal services. Any comments made by a manager or legal representative should be entered into the application for authorisation. Notes of all the discussions should be kept and retained on file.

4.3.2 The Codes of Practice advise that Authorising Officers should not be directly responsible for authorising investigations or operations in which they are directly involved although it is recognised that this may sometimes be unavoidable. This is highly unlikely however. Legal advice together with advice from the Authorising Officer's senior line manager should take place before any authorisation is signed in these circumstances.

4.3.3 If an Investigating Officer intends to carry out DS or use CHIS they should complete and submit an "Application for Directed Surveillance" form which is marked as such, or an "Application for the use of CHIS" to an Authorising Officer. An electronic version of the most up-to-date forms and Codes of Practice are available online downloaded from the Home Office in **Appendix B**. The Investigating Officer should also consider including an assessment of the risk of collateral intrusion and detail any measures taken to limit this.

4.3.4 **Appendix C** shows the steps which are required as part of the authorisation process and the Covert Surveillance and Property Interference Revised Code of Practice (August 2018) contains best practice guidelines with regard to applications for

Directed Surveillance including the need for information to be presented in a fair and balanced way.

4.3.5 The person seeking the authorisation should obtain a Unique Reference Number from the RIPA Co-ordinator and complete parts 1 and 2 of the form having regard to the guidance given in this Guide and the statutory Codes of Practice.

4.3.6 The form should then be submitted to the Authorising Officer for authorisation.

**4.4 Authorising Officers - What they must do before authorising surveillance**

4.4.1 Before giving authorisation, an Authorising Officer **must** be satisfied that the reason for the request is the permitted reason under the Act and permitted under the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, i.e.

- in the case of directed surveillance, for the purpose of the prevention and detection of conduct which constitutes one or more criminal offences that are:

  (i) punishable by a maximum term of at least 6 months imprisonment; or

  (ii) are offences under:

  a. Section 146 of the Licensing Act 2003 (sale of alcohol to children)
  b. Section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
  c. Section 147A of the Licensing Act 2003 (persistently selling alcohol to children); or
  d. Section 7 of the Children and Young Persons Act 2003 (sale of tobacco etc. to persons under eighteen); and

or

- in the case of CHIS, for the purpose of the prevention and detection of crime or for the preventing of disorder;

and

e. the desired result of the covert surveillance cannot reasonably be achieved by other means;

and

f. the risks of collateral intrusion (the risk of obtaining private information about persons who are not the subject of investigation) have been properly considered, and the reason for the surveillance is balanced proportionately against the risk of collateral intrusion with particular consideration given to cases where religious, medical, journalistic or legally privileged material may be inferred or where communications between a Member of Parliament and another person on constituent business may be involved.

and

g. there must also be consideration given to the possibility of collecting confidential personal information. If there is a possibility of collecting personal information the matter should be passed to the Senior Responsible Officer for consideration.

4.4.2 An Authorising Officer **must** also be satisfied that the surveillance in each case is

**necessary** and **proportionate**.

This is defined as:-

**Necessity**

- Obtaining an authorisation under the 2000 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

- The 2000 Act first requires that the person granting an authorisation for directed surveillance believes that the authorisation is necessary in the circumstances of the particular case for the statutory ground in section 28(3)(b) of the 2000 Act being *"for the purpose of preventing or detecting crime or of preventing disorder"* .

**Proportionality**

- The following elements of proportionality should be considered:

  i) balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;

  ii) explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

  iii) considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;

  iv) evidencing as far as reasonably practicable, what other methods have been considered and why they were not implemented, or have been implemented unsuccessfully.

When the Authorising Officer has considered if the surveillance is necessary and proportionate they must complete the relevant section of the form explaining why in his/her opinion the surveillance is necessary and proportionate.

## 4.5 Judicial Approval

4.5.1 From 1 November 2012, any DS or CHIS authorisation granted by an Authorising Officer **does not** take effect until an order has been made by a Justice of the Peace ("Magistrate") approving the grant of the authorisation.

4.5.2 When an authorisation has been granted by an Authorising Officer (following the process set out above) and after consultation with Legal Services, an Officer authorised by the Council to appear on its behalf in Magistrates' Court proceedings (the "Applicant") needs to make an application to the Magistrates' Court for judicial approval of the authorisation before the authorisation can take effect (i.e. before lawful surveillance can begin). These steps will be taken by Legal Services. The Investigating Officer will however be asked to attend court when the application is heard.

4.5.3 Under the Criminal Procedure Rules 2012, the Applicant must:

(i) apply in writing and serve the application on the appropriate court officer;

(ii) attach the authorisation which the Applicant wants the court to approve (NB the original authorisation should be shown to and a copy provided to, the Magistrate. The original authorisation should be retained by the Investigating Officer) ;

(iii) attach such other material (if any) on which the Applicant is relying to satisfy the court that the authorisation was necessary for the purposes of the prevention and detection of crime and was proportionate (as set out in paragraph 4.4.1) and that the authorisation was granted by a person designated for the purposes of RIPA .

The Applicant should also provide the Magistrate with two copies of a partially completed judicial application/order to assist the process.

4.5.4 The hearing will be in private and heard by a single District Judge/JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters. The forms and supporting papers must, by themselves, make the case. It is not sufficient to provide oral evidence where this is not reflected or supported in the papers provided. The JP may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.

4.5.5 The relevant Magistrate may approve the granting of a DS authorisation if, and only if, they are satisfied that:

(i) at the time of the grant (i.e. when approval was given by the Authorising Officer):

a. there were reasonable grounds for believing that the authorisation was necessary for the purposes of the prevention and detection of crime and was proportionate (as set out in paragraph 4.4.1); and

b. that the authorisation was granted by a person designated for the purposes of authorising DS; and

(ii) at the time when the relevant Magistrate is considering the matter, there remain reasonable grounds for believing that the authorisation is necessary and proportionate (as set out in paragraph 4.4.1)

4.5.6 The relevant Magistrate may approve the granting of a CHIS authorisation if, and only if, they are satisfied that:

(i) at the time of the grant (i.e. when approval was given by the Chief Executive)

a. there were reasonable grounds for believing that the authorisation was necessary for the purposes of the prevention and detection of crime or disorder and was proportionate (as set out in paragraph 4.4.1) and that the arrangements set out in paragraph 3.2.3, together with any other prescribed requirements, were in place; and

b. that the authorisation was granted by a person designated for the purposes of authorising CHIS, and

(ii) at the time when the relevant Justice of the Peace is considering the matter, there remain reasonable grounds for believing that the authorisation is necessary and proportionate (as set out in paragraph 4.4.1)

4.5.7 Where an application is approved by a Magistrate, the Investigating Officer should:

(i) retain a copy of the judicial application/order that has been signed by the Magistrate;

(ii) retain the original authorisation; and

(iii) notify the RIPA Co-Ordinator of the Court's approval for the authorisation and provide a copy of the authorisation, application and Order for the RIPA records.

4.5.8 Where an application is not approved by a Magistrate, the authorisation does not take effect and the surveillance proposed in the authorisation must not be carried out.

4.5.9 Where an application is refused by a Magistrate, the Magistrate may make an order quashing the authorisation.

## 5. Record Keeping, Duration, Review, Errors, Renewal and Cancellation of Authorisations and Errors

### 5.1 Record Keeping

5.1.1 A record of all authorisations should be centrally retrievable within the Council for a period of at least three years and should be regularly updated and made available to the Investigatory Powers Commissioner and inspectors upon request. This record should contain the information outlined within the Covert Surveillance and Property Interference Revised Code of Practice (August 2018).

5.1.2 The Central Record should contain the following:-

The type of authorisation.

The date of the authorisation.

Name and rank of the Authorising Officer

The Unique Reference Number (URN) of the investigation or operation.

The title of the investigation or operation, including a brief description and names of subjects, if known.

Details of any renewal of the authorisation.

Whether the investigation or operation is likely to result in obtaining confidential information.

The date the authorisation was cancelled.

Full details of any equipment to be used

### 5.2 Duration

5.2.1 DS authorisations will cease to have effect after **three months** from the date of judicial approval unless renewed (also subject to judicial approval) or cancelled.

5.2.2 Authorisations should be given for the maximum duration (i.e. three months) but reviewed on a regular basis and formally cancelled when no longer needed.

5.2.3 CHIS authorisations will cease to have effect **after twelve months** from the date of approval. However, if using a juvenile CHS, the authorisation lasts for one month only but can be reviewed and renewed with court approval. For CHIS authorisations, legal advice must be sought.

5.2.4 Investigating Officers should indicate within the application the period of time that they estimate is required to carry out the surveillance, this will be proportionate to the objectives of the investigation and give due consideration to collateral intrusion.

5.2.5 The authorising officer must give authorisations in writing, except in urgent cases when they may be given orally by the authorising officer. An urgent case for oral authorisation should only be made if the applicant believes that the time required for an authorising officer to grant a written authorisation would, in the applicant's judgement, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being sought. An urgent oral authority lasts 72 hours from the time the surveillance was first authorised, unless renewed. .

5.2.7 It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

**5.3 Review**

5.3.1 An Investigating Officer must carry out a **regular** review of authorisations. If an authorisation is no longer required it **must** be cancelled.

5.3.2 The results of any review must be included on the review form (see forms Review of Directed Surveillance" and "Review of CHIS" available from the RIPA Co-ordinator, or the Home Office website address given in **Appendix B**).

5.3.3 The Authorising Officer also has a duty to review authorisations that have been granted when it is necessary or practicable to do so. Particular attention should be given to authorisations involving collateral intrusion or confidential material.

5.3.4 The Authorising Officer should keep a copy of the review form for at least 3 years and a copy should be given to the Investigating Officer. A copy of the review form must also be sent to the RIPA Co-ordinator.

**5.4 Renewals**

5.4.1 An Investigating Officer can ask for, and an Authorising Officer can grant, subject to judicial approval, a renewal of an authorisation before it would cease to have effect and not more than 7 days before the original authorisation is due to expire.

5.4.2 A renewal can last for up to three months, effective from the date that the previous authorisation would cease to have effect. A renewal may also be granted for urgent cases for 72 hours.

5.4.3 An Authorising Officer can grant more than one renewal, subject to judicial approval, as long as the request for authorisation still meets the requirements for authorisation. An Authorising Officer must still consider all of the issues that are required for a first application before a renewal can be granted.

5.4.4 If the reason for requiring authorisation has changed from its original purpose it will not be appropriate to treat the application as a renewal. It should be treated as a new authorisation request. The original authorisation should be cancelled and a new authorisation should be sought, granted by an Authorising Officer and approved by a Magistrate.

5.4.5 All applications for renewal of authorisations for directed surveillance should include:

Whether this is the first renewal.
Every occasion on which the authorisation has been renewed previously.
Significant changes to the information relating to the conduct to be authorised and also the purpose of the investigation or operation.
The reasons why it is considered to be necessary and proportionate to continue with the directed surveillance
The content and value to the investigation or operation of the information so far obtained by the surveillance and the result of regular reviews of the investigation operation

5.4.6 An application for a renewal must be completed on the appropriate form (see forms "Renewal of Directed Surveillance" and "Renewal of CHIS" available from the RIPA Co-ordinator, or the Home Office website address given in **Appendix B**).

5.4.7 The Authorising Officer should keep a copy of the renewal and a copy should be given to the Investigating Officer. A copy of the renewal form, judicial application and order must also be sent to the RIPA Co-ordinator.

### 5.5 Cancellations

5.5.1 If the reason for requiring the authorisation no longer exists, the authorisation must be cancelled and in any event as soon as the operation for which an authorisation was sought ceases to be necessary or proportionate by the Authorising Officer. This applies to both original applications and renewals (see forms "Cancellation of Directed Surveillance" and "Cancellation of CHIS" available from the RIPA Co-ordinator, or the Home Office website address given in **Appendix B**).

5.5.2 Authorisations must also be cancelled if the surveillance has been carried out and the original aim has been achieved. Authorising Officers will ensure that authorisations are set to expire at the end of the appropriate statutory period.

5.5.3 It is the responsibility of the Investigating Officer to monitor their authorisations and seek cancellation of them where appropriate.

5.5.4 The Authorising Officer should keep a copy of the cancellation form and a copy should be given to the Investigating Officer. A copy of the cancellation form must also be sent to the RIPA Co-ordinator.

### 5.6 Errors in applications

5.6.1 An error must be reported if it is a "relevant error" to the Investigatory Powers Commissioner as soon as reasonably practicable. If the error is of a serious nature then the Commissioner may require that the person concerned (i.e. who you intended to monitor) is informed of the error. They will consider the seriousness of the error and the potential impact on the person involved ie under surveillance.
Legal advice should be sought as soon as possible if errors are identified

### 5.7 Review of Policy and Procedure

The Council's Audit and Governance Committee will receive annual reports on the use of RIPA including the use of RIPA by the Authority.

## 6. The RIPA Co-ordinator

### 6.1 Role

The RIPA Co-ordinator will:-

(i) provide a Unique Reference Number for each authorisation sought;

(ii) keep copies of the forms for a period of at least three years;

(iii) keep a register of all of the authorisations, reviews, renewals and cancellations, including authorisations granted by other public authorities relating to joint surveillance by the Council and that other public authority;

(iv) provide administrative support and guidance on the processes involved;

(v) monitor the authorisations, reviews, renewals and cancellations so as to ensure consistency throughout the Council;

(vi) monitor each department's compliance and act on any cases of non-compliance;

(vii) provide training and further guidance on and awareness of RIPA and the provisions of this Guide; and

(viii) review the contents of the Guide, in consultation with Investigating Officers, Authorising Officers and the Senior Responsible Officer.

All original applications for authorisations and renewals including those that have been refused must be passed to the RIPA Co-ordinator as soon as possible after their completion with copies retained by the Authorising Officer and the Investigating Officer.

The RIPA Co-ordinator shall be either of the people in post of Principal Legal Officer.

All cancellations must also be passed to the RIPA Co-ordinator.

6.2 It is however the responsibility of the Investigating Officer, the Authorising Officers and the Senior Responsible Officer to ensure that:-

(i) authorisations are only sought and given where appropriate;

(ii) authorisations are only sought and renewed where appropriate;

(iii) authorisations are reviewed regularly;

(iv) authorisations are cancelled where appropriate; and

(v) they act in accordance with the provisions of RIPA.

## 7. Legal Advice

Legal Services will provide legal advice to staff making, renewing or cancelling authorisations, including making applications for judicial approval.

## 8. Joint Investigations/Collaborative working

Where joint investigations are carried out with other agencies, such as the Department of Work and Pensions (DWP) or the Police, the RIPA Co-ordinator

should be notified of the joint investigation and provided with a copy of any RIPA authorisation granted by another agency in respect of a joint investigation involving Council officers.

Any person granting or applying for an authorisation will need to be aware of the particular sensitivities in the local community where the surveillance is taking place.

Where possible, public authorities should try to avoid duplication of authorisations as part of a single investigation or operation. Where two agencies are conducting directive or intrusive surveillance as part of a joint operation, only one authorisation is required. Be cautious however of undertaking any form of surveillance that the Council is not authorised to do under another Authorities authorisation.

## 9. National Anti-Fraud Network (NAFN)

9.1 Since September 2014, Local Authorities can only access communications data via the National Anti-Fraud Network (NAFN). 'NAFN is a not-for-profit, non-incorporated body formed by its members to provide services which support their work in the protection of the public purse. Established in 1997, NAFN was created as a centre of excellence to provide data and intelligence to its members. This includes assisting members in the provision of effective corporate and financial governance. NAFN works with its members and other stakeholders to enhance and expand its range of services. It maintains all data in a secure and confidential environment conforming to Government legislation and national best practice

9.2 The Council is a member of NAFN. We must remain a paid up member in order to make use of its single point of contact (SPoC) service in relation to communications data.

9.3 The Council is a member, primarily to make use of other services provided by NAFN (credit referencing, DVLA checks, debtor tracing etc.) but given that Officers could now utilise the RIPA SPoC service and obtain communications data, guidance needs to be in place to govern the process.

9.4 This procedural guide is based on the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office Code of Practice on the Acquisition and Disclosure of Communication Data. The Council takes responsibility for ensuring its RIPA procedures are continuously improved and asks that any Officers with suggestions contact the RIPA Coordinator in the first instance. If any of the Home Office Codes of Practice change, the appropriate guide will be updated, and the amended version placed on the internet / published accordingly. Regular training sessions will also be provided to ensure that staff members are fully conversant with the Act

## 10. Complaints

The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against a public authority use of investigatory powers. It is the only appropriate tribunal for human rights claims against the intelligence services. All complaints for the use of powers should be directed to the IPT.

# Notes and definitions

Superscript notes:

1. Wherever in this document the word Policy and/or Guide is used; this applies to this whole document and is the Council's RIPA Policy.

2. Complete dates on when Policy is adopted and then dates of each review.

**APPENDIX A**

# OFFICERS

The following officers are the Senior Authorising Officer and the Authorising Officers for the purposes of RIPA.

| |
|---|
| **Senior Responsible Officer**<br><br>Sanjiv Kohli - Deputy Chief Executive. Director of Resources. S151 officer |
| **Authorising Officers – Directed Surveillance** |
| Matthew Finch- Director of Communities and Environment<br><br>Matt Lamb –Director of Growth and Regeneration |
| **Authorising Officer – CHIS**<br><br>Chief Executive – John Robinson |
| **RIPA Co-Ordinator –** Principal Legal Officer and Deputy Monitoring Officer– Lisa Ingram |

**APPENDIX B**

## AUTHORISATION FORMS

All of the forms necessary for RIPA are available from the Home Office website.
These forms are a mandatory part of the process and must be used in line with the guidance.

**All decisions about using regulated investigatory powers must be recorded as they are taken on the required form.**

This is the case for applicants seeking authority to undertake regulated conduct and for Authorising Officers and designated persons who consider and decide whether to grant authority or give notice for that conduct. Select the form that you require from the hyperlinked lists below:-

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

### Directed Surveillance

Application for DS

- https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance

Renewal form form DS

- https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance

Review of use of DS

- https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance

Cancellation

- https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form

### Covert Human Intelligence Sources

**Application CHIS**

- https://www.gov.uk/government/publications/application-for-the-use-of-covert-human-intelligence-sources-chis

Review CHIS

- https://www.gov.uk/government/publications/reviewing-the-use-of-covert-human-intelligence-sources-chis

### Reporting errors to the IPCO

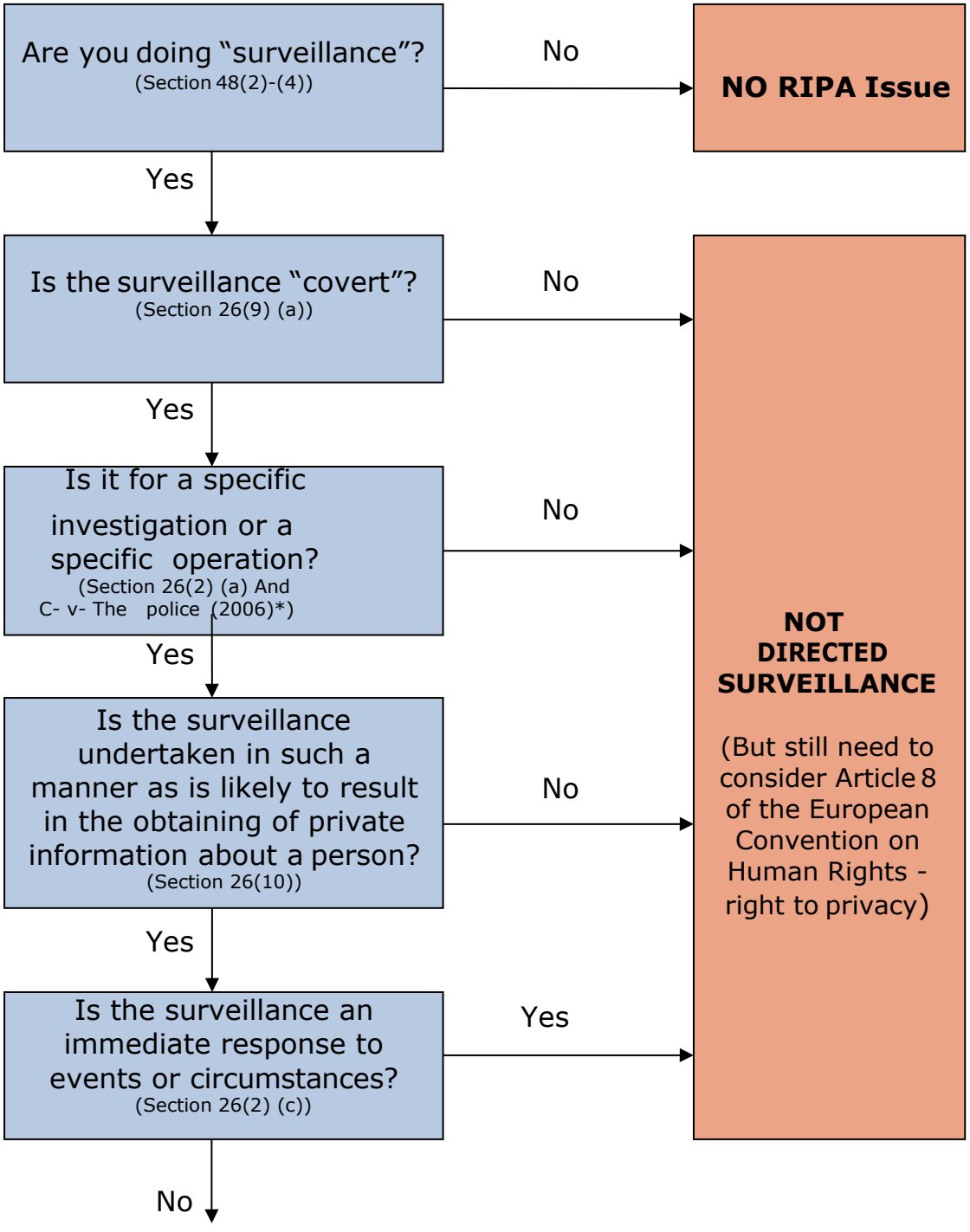
**https://www.ipco.org.uk/what-we-do/errors/**

## FLOWCHARTS

**Appendix C**

**Flowchart 5.1 - Are you doing Directed Surveillance?**

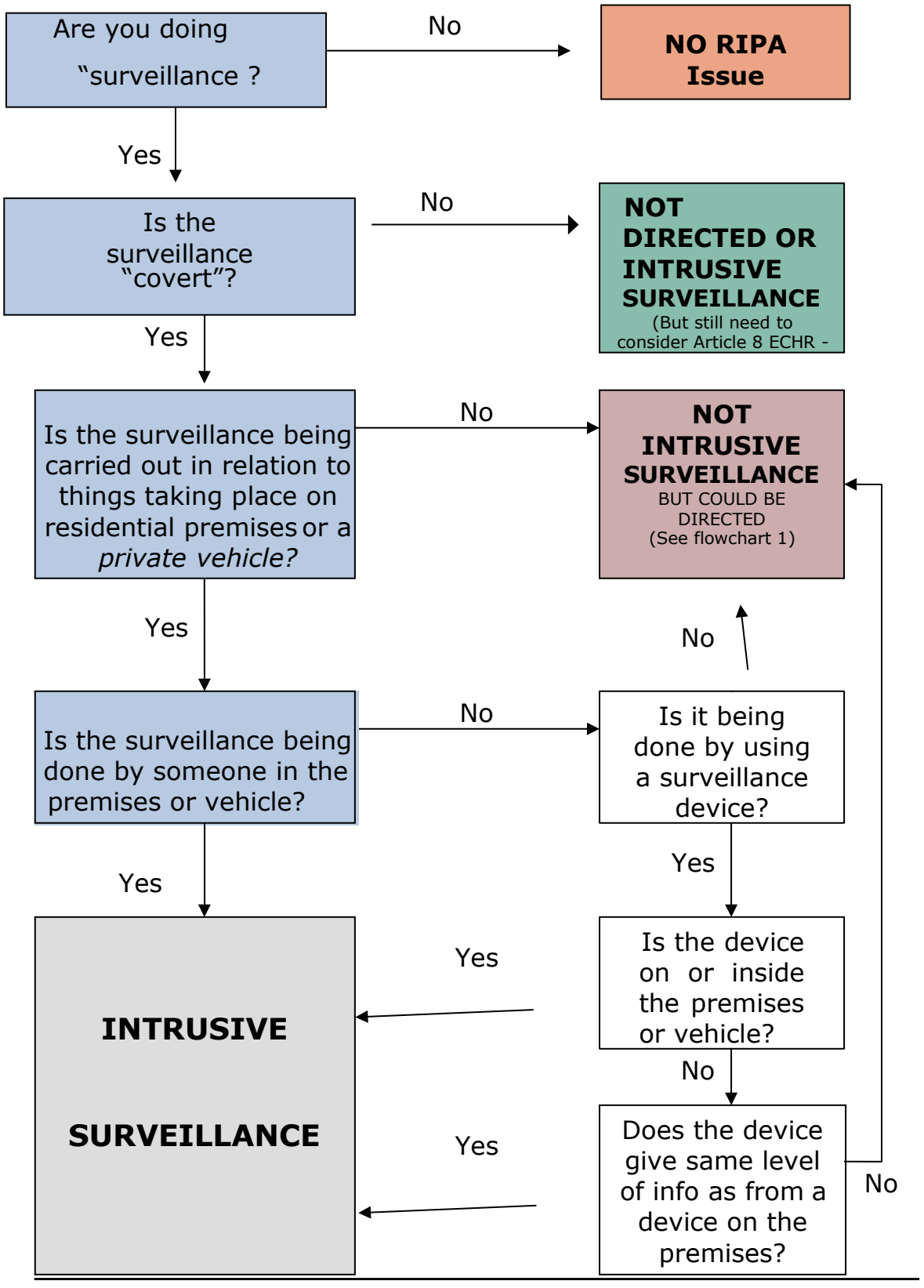
*All references are to sections of the Regulation of Investigatory Powers Act 2000*



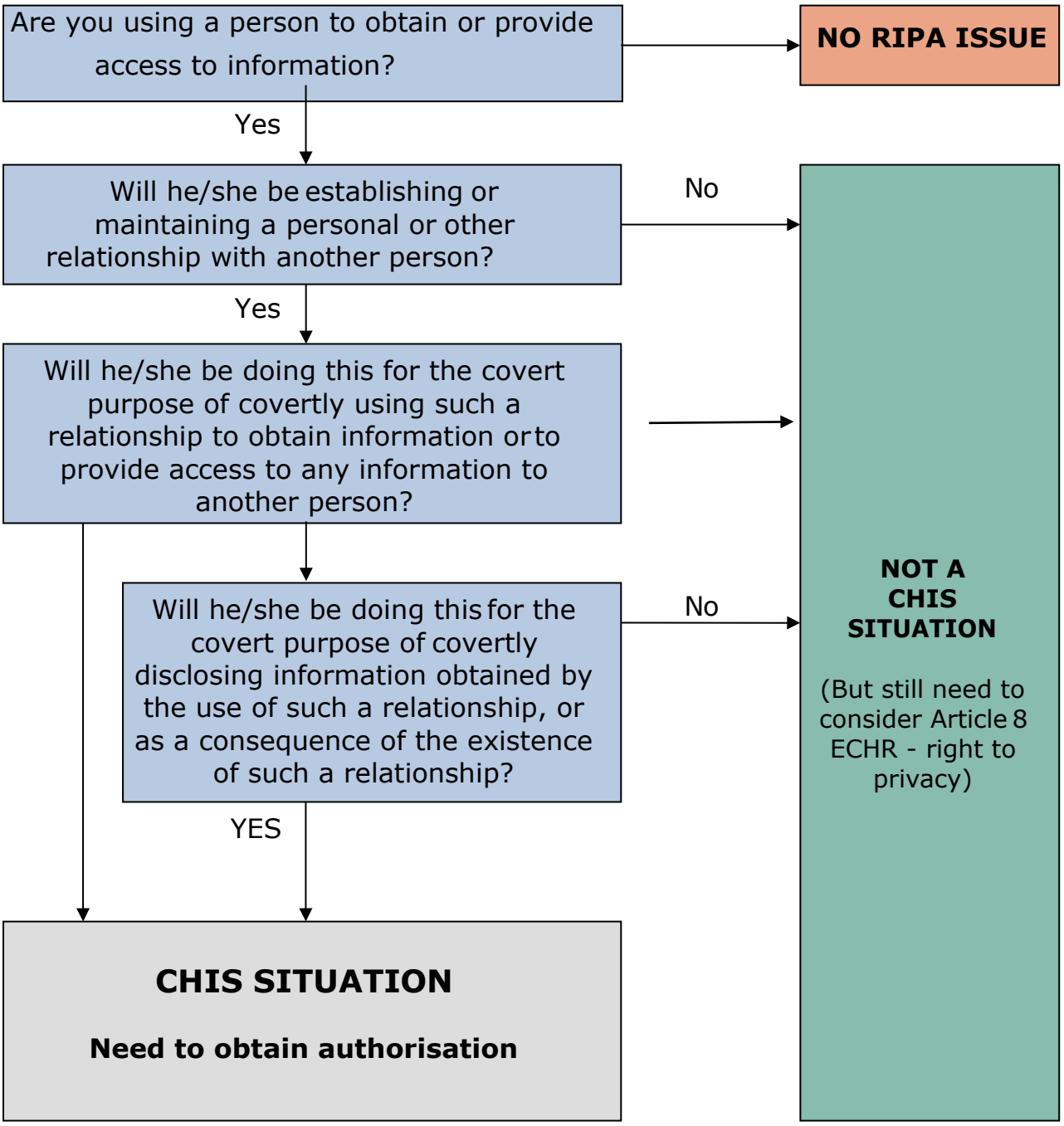

**DIRECTED SURVEILLANCE**

(Also consider if Intrusive Surveillance too – check flowchart 2)

**Flowchart 5.2 -Are you doing Intrusive Surveillance?**

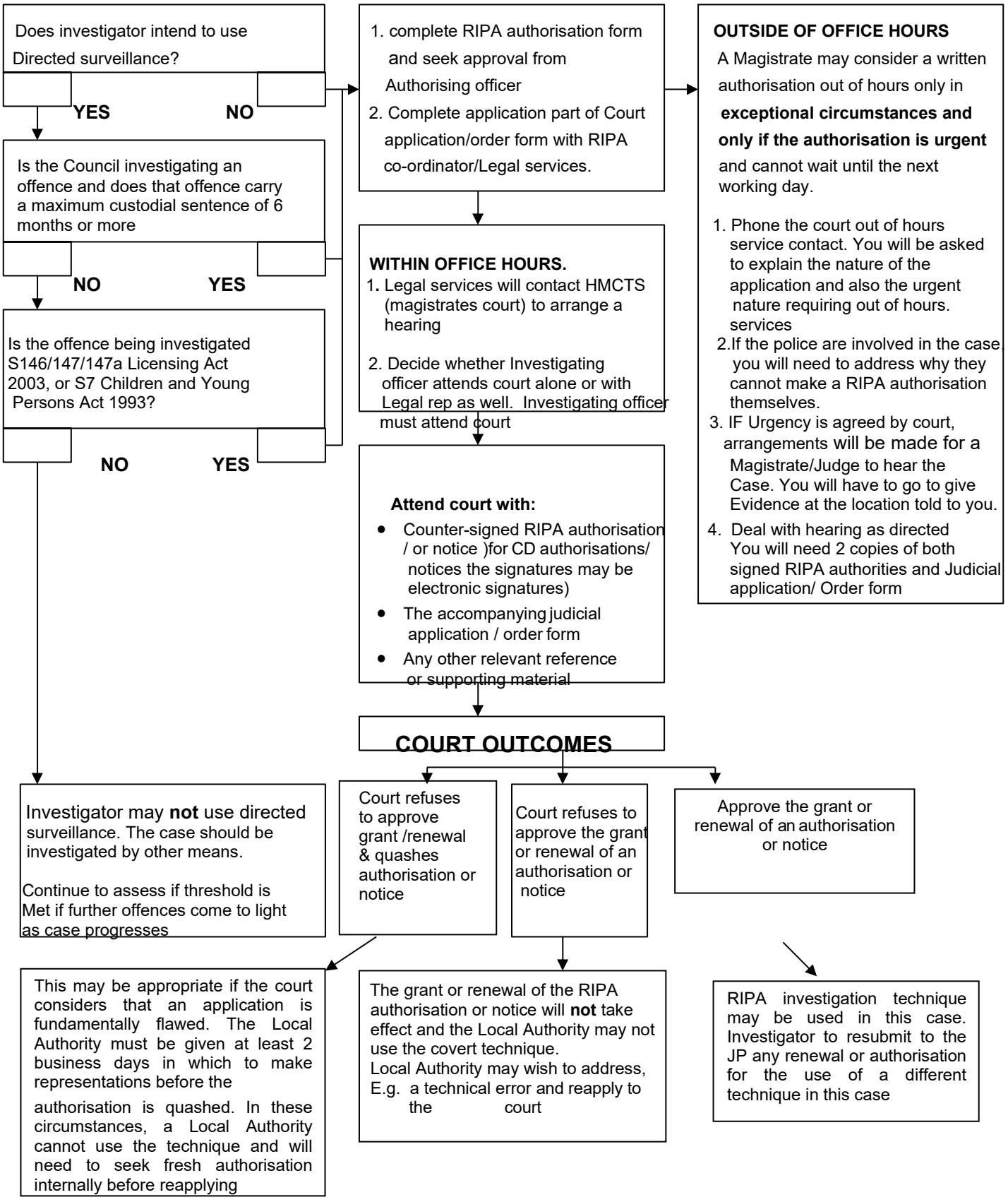


**Flowchart 5.3 - Are you using CHIS? (Section 26(8)**



**Appendix D**

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




Obtain signed order and retain original RIPA authorisation / notice. – Ensure copy is given to Legal Services Ripa Co-ordinator. For CD authorisations or notices, Council investigator to provide an additional copy of the judicial order to the SPoC. If out of hours a copy of the signed order is to be provided to the relevant court the next working day.

# CODES OF PRACTICE

https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2022
https://www.gov.uk/government/publications/equipment-interference-code-of-practice--2
https://assets.publishing.service.gov.uk/media/5a8080a540f0b62305b8b86e/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf
https://www.gov.uk/government/publications/covert-human-intelligence-sources-code-of-practice-2022
https://www.gov.uk/government/publications/code-of-practice-for-investigation-of-protected-electronic-information