Northumberland
County Council

Policy

Authorisation and conduct of surveillance. (Regulation of Investigatory Powers Act 2000)

Summary

Northumberland County Council is charged with carrying out various enforcement duties which require officers to conduct appropriate investigations. On occasion, these investigations will require officers to gather information using covert surveillance techniques such as:

- *Directed surveillance.*
- The use of an informant or an officer working undercover (known as a '*Covert Human Intelligence Source*' or '*CHIS*').

Investigations that require such surveillance and the use of an informant are governed by the *Regulation of Investigatory Powers Act 2000 ('RIPA')* as it is necessary to strike a balance between the public interest and the rights of individuals.

To conduct any covert surveillance techniques, there is a strict application process known as an authorisation, specially trained officers within the Council can grant authorisations, provided certain legal tests are met and then judicial approval is also required.

This Policy sets out the Council's approach to covert investigation techniques and the purpose of this Policy is to ensure that the Council complies with RIPA and associated guidance or Codes of Practice in accordance with the principles of consistency, balance and fairness.

Adopted by the Council: XX 2024

Reviewed:

Contents

1 Introduction

1.1 Northumberland County Council ('*the Council*') is charged with carrying out various enforcement duties which require officers to conduct appropriate investigations.

1.2 Occasionally, investigations will require such officers to gather information in respect of individuals who may be unaware of what is taking place.

1.3 This may be by the use of covert surveillance or, more rarely, by using an informant or an officer working undercover (known as a '*Covert Human Intelligence Source*' or '*CHIS*').

1.4 In conducting these investigations, it is necessary to strike a balance between the public interest and the rights of individuals.

1.5 This Policy sets out the Council's approach to covert investigation techniques within the framework of the *Regulation of Investigatory Powers Act 2000* ('*RIPA*').

1.6 The purpose of this Policy is to ensure that the Council complies with RIPA and associated guidance or codes of practice in accordance with the principles of consistency, balance and fairness.

1.7 Any queries concerning the content of the document should be addressed to the RIPA Monitoring Officer.

2 RIPA

2.1 The purpose of RIPA

2.1.1 RIPA provides a legal framework for the control and regulation of surveillance and information techniques which eligible public authorities under RIPA ('*Public Authorities*') undertake as part of their duties.

2.1.2 The need for such control arose as a result of Article 8 of the *European Convention on Human Rights* (as set out in Schedule 1 to the *Human Rights Act 1998*), which states as follows:

Article 8

Right to respect for private and family life

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 well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

2.1.3 The right under paragraph 1 of Article 8 is a qualified right and Public Authorities may interfere with this right for the reasons given in

paragraph 2, and RIPA provides the legal framework for lawful interference.

2.2 **The scope of this Policy**

2.2.1 This Policy is intended to cover the surveillance and information gathering techniques which are most likely to be carried out by the Council.

2.2.2 Neither RIPA itself nor this Policy covers the use of any overt surveillance, or circumstances where members of the public volunteer information to the Council.

2.2.3 RIPA does not normally cover the use of overt CCTV surveillance systems but if any officer envisages using any such system for surveillance, they should first contact the RIPA Monitoring Officer for advice in that respect.

2.2.4 RIPA (and subsequent legislation within the Investigatory Powers Act 2016 which replaced its provisions in relation to interception and acquisition of communications data) deals with a wide variety of surveillance techniques. Examples of those which **cannot** or **will not** be used by local authorities include:

(a) The interception of any communication, such as postal, telephone or electronic communications without both the sender and receiver's permission;

(b) The acquisition and disclosure of information to who has sent or received any postal, telephone or electronic communication; and

(c) 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 ('Intrusive Surveillance').

2.3 **The consequences of not following RIPA**

2.3.1 *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.

2.3.2 Lawful surveillance is exempted from civil liability – if officers follow this Policy, then they should be protected by this '*RIPA Shield*'.

2.3.3 Not obtaining valid authorisation may have the following consequences:

(a) The evidence that is gathered may be inadmissible in Court;

(b) The subjects of surveillance can bring their own proceedings against the Council, or defeat proceedings brought by the Council against them on human rights grounds, i.e., that we have infringed their rights under Article 8 but have failed to ensure that we are protected by the RIPA Shield;

(c) Where a challenge under Article 8 is successful the Council may be liable to pay financial compensation;

(d) A complaint may be made to *The Investigatory Powers Commissioner's Office* ('*IPCO*') and

(e) Any person who believes that their rights have been breached can have their complaint dealt with by *the Investigatory Powers Tribunal* (https://www.ipt-uk.com/).

2.4 The Investigatory Powers Commissioner's Office

2.4.1 IPCO provides independent oversight of the use of investigatory powers by intelligence agencies, the police and other Public Authorities.

2.4.2 It has unfettered access to all locations, documentation and information systems as necessary to carry out full functions and duties and will review the way in which Public Authorities implement the requirements of RIPA.

2.4.3 The Council will receive periodic inspections from IPCO, during which it will check to see whether the Council is complying with RIPA.

2.4.4 It is important that the Council is able to demonstrate that it complies with both the provisions of RIPA and of this Policy.

3 Covert surveillance

3.1 Categories of covert surveillance

3.1.1 Surveillance includes:

(a) Monitoring, observing or listening to persons and their movements, conversations and other activities;

(b) Recording anything monitored, observed or listened to in the course of surveillance; and

(c) The use of a surveillance or recording device such as a camera, camcorder, binoculars, CCTV, mobile phone, etc.

3.1.2 Surveillance is covert if the persons who are the subject of the surveillance are unaware that it is taking place.

3.1.3 There are three categories of covert surveillance under RIPA:

(a) ***Directed surveillance*** (*section 28* of RIPA);

(b) The use of a ***Covert Human Intelligence Source*** ('*CHIS'*) (*section 29* of RIPA); and

(c) ***Intrusive surveillance*** (*section 32* of RIPA).

PLEASE NOTE – the Council **cannot** and **will not** issue authorisations for intrusive surveillance.

3.2 Directed Surveillance ('*DS*')

3.2.1 Surveillance is Directed Surveillance within the meaning of RIPA if it is covert but not intrusive and is undertaken:

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

(b) in such a manner as is likely to result in the obtaining of

private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

3.3 **Covert Human Intelligence Source** (‘*CHIS*’)

3.3.1 A CHIS includes:

(a) an officer who establishes or maintains a personal or other relationship with a person for the covert purpose of using the relationship to obtain information (e.g., an officer who is working undercover); and

(b) any other person who establishes such a relationship for the covert purpose of disclosing information obtained by the use of the relationship (e.g., an informant).

3.3.2 A purpose is covert if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

3.3.3 In either case set out in paragraph 3.3.1 above there is a need to consider the safety and welfare of the CHIS, and the identity of the CHIS must always be kept private and protected.

3.4 **Intrusive Surveillance**

3.4.1 In broad terms, Intrusive Surveillance means surveillance carried out on residential premises or in a private vehicle, either by means of an individual present on the premises or in the vehicle, or by means of a surveillance device.

3.4.2 Local authorities are **not** permitted to carry out intrusive surveillance.

4 <u>Procedure for Obtaining Authorisations</u>

4.1 **The Senior Responsible Officer** (‘*SRO*’)

4.1.1 The Council’s SRO (in conjunction with the RIPA Monitoring Officer as set out below) is responsible for:-

(a) ensuring the integrity of the Council’s RIPA processes;

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

(c) oversight of reporting errors to the IPCO and implementing processes to minimise repetition of errors;

(d) engaging with IPCO for inspections;

(e) overseeing the implementation of any post-inspection plans; and

(f) ensuring that all Authorising Officers receive appropriate

training.

4.2 **The RIPA Monitoring Officer (Monitoring Officer)**

4.2.1 In accordance with the constitution of the Council, the Monitoring Officer is also responsible for:-

(a) ensuring the integrity of the operation of RIPA

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

(c) oversight of reporting errors to the IPCO and implementing processes to minimise repetition of errors;

(d) engaging with IPCO for inspections and overseeing the implementation of any post-inspection plans;

(e) Monitoring authorisations and conducting reviews of applications, authorisations and refusals and reviewing renewals and cancellations.

4.3 **Authorising Officers**

4.3.1 Authorising Officers may authorise, review or cancel DS, and may authorise, review or cancel the use of a CHIS.

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

Appendix A sets out the officers within the Council who may grant authorisations.

Authorisations must be given in writing by the Authorising Officer.

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

4.4 **Investigating Officers** - *What they must do before applying for authorisation*

4.4.1 Investigating Officers should think about the need to undertake DS or using a CHIS before they seek authorisation.

Investigating Officers 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 beforehand. Any comments by a supervisor should be entered into the application for authorisation.

4.4.2 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.

4.4.3 If an Investigating Officer intends to carry out DS or use CHIS, they

should complete and submit an ***Application for Directed Surveillance*** form, or an ***Application for CHIS*** (as the case might be) to an Authorising Officer.

4.4.4 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**.

4.4.5 The Investigating Officer should also include an assessment of the risk of collateral intrusion to the privacy of third parties and detail any measures taken to limit this.

4.4.6 **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 DS, including the need for information to be presented in a fair and balanced way.

4.4.7 The person seeking the authorisation should obtain a *Unique Reference Number* from the RIPA Monitoring Officer and complete parts 1 and 2 of the form, having regard to the guidance given in this Policy and the statutory Codes of Practice.

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

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

4.5.1 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, i.e., in the case of DS, for the purpose of the prevention and detection of conduct which constitutes one or more criminal offences that are:

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

(b) are offences under:

(i) *section 146* of the *Licensing Act 2003* (sale of alcohol to children);

(ii) *section 147* of the *Licensing Act 2003* (allowing the sale of alcohol to children);

(iii) *section 147A* of the *Licensing Act 2003* (persistently selling alcohol to children); or

(iv) *section 7* of the *Children and Young Persons Act 1993* (sale of tobacco etc. to persons under eighteen);

(v) *section 91 of the Children and Families Act 2014* (purchase of tobacco, nicotine products on behalf of persons under 18etc)

(vi) *section 92 of the Children and Families Act 2014 (prohibition of the sale of nicotine products to persons under 18)*

AND

(c) that the desired result of the covert surveillance cannot reasonably be achieved by other means; and

(d) that the risks of collateral intrusion (meaning 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

(e) that there must also be consideration given to the possibility of collecting confidential personal information, in which case the matter should be passed to the SRO for consideration.

4.4.2 An Authorising Officer **must** also be satisfied that the surveillance in each case is **necessary** and **proportionate**. (The Protection of Freedoms Act 2012)

4.4.3 In determining whether the surveillance is necessary and proportionate, the considerations detailed below should be taken into account.

4.4.4 **Necessity**

(a) Obtaining an authorisation under RIPA 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.

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

4.4.5 **Proportionality**

(a) 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; and

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

(b) When the Authorising Officer has considered whether the surveillance is necessary and proportionate, they must complete the relevant section of the form explaining why in their opinion the surveillance is necessary and proportionate.

4.5 **Judicial approval (Magistrates' Court)**

4.5.1 **Any DS or CHIS authorisation granted by an Authorising Officer does not take effect until an Order has been made by the Magistrates' Court approving the grant of the authorisation**.

4.5.2 When an authorisation has been granted by an Authorising Officer, a duly authorised officer of the Council (i.e., someone with valid written authorisation from the Council to appear on its behalf in Magistrates' Court proceedings) ('*the Applicant*') must make an application to the Court for judicial approval of the authorisation before the authorisation can take effect (i.e. before lawful surveillance may begin).

Before making an application, it is sensible to seek advice from Legal Services (Regulation Team) as to the content of an application and arranging the listing of the application as listing is now dealt with at a central location in the North Northumbria Region. Please use the email address below to contact the Regulation Team.

regulation-prosecution@northumberland.gov.uk

4.5.3 In accordance with the *Criminal Procedure Rules 2020*, (Rule 47) the Applicant must:

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

(b) attach the authorisation which the Applicant wants the court to approve (NB: the original authorisation should be shown, and a copy of it provided, to the Court, with the original being retained by the Investigating Officer);

(c) 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 above) and that the authorisation was granted by a person properly designated for the purposes of exercising the powers under RIPA; and

(d) the Applicant should also provide the Court with two copies of a partially completed judicial application/Order to assist the process.

(e) The Court may approve the granting of a DS authorisation if, and only if, it is satisfied that:

(i) at the time that approval was given by the Authorising Officer):

- there were reasonable grounds for believing that the authorisation was necessary for the purposes of the prevention and detection of crime and was proportionate; and

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

(ii) at the time when the Court is considering the matter, there remains reasonable grounds for believing that the authorisation is necessary and proportionate.

4.5.4 The Court may approve the granting of a CHIS authorisation if, and only if, it is satisfied that:

(a) at the time that approval was given by the Council's Head of Paid Service):

(i) 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, and that the arrangements set out in this Policy, together with any other prescribed requirements, were in place; and

(ii) that the authorisation was granted by a person designated for the purposes of authorising CHIS, and

(b) at the time when the Court is considering the matter, there remains reasonable grounds for believing that the authorisation is necessary and proportionate.

4.5.5 Where an application is approved by the Court, the Investigating Officer should:

(a) retain a copy of the judicial application/Order that has been signed on behalf of the Court;

(b) retain the original authorisation; and

(c) notify the RIPA Monitoring Officer of the judicial approval for the authorisation and provide a copy of the authorisation, application and Order for the RIPA records.

4.5.6 Where an application is not approved by the Court, the authorisation does not take effect and the surveillance proposed in the authorisation cannot be carried out.

4.5.7 Where an application is refused by the Court it may make an Order quashing the authorisation.

5 Record keeping, duration, review, renewal & cancellation of authorisations, and errors

5.1 Record Keeping

5.1.1 A record of all authorisations will be centrally retrievable within the Council for a period of at least 3 years and will be regularly updated and made available IPCO and its inspectors upon request.

5.1.2 This record should contain the information outlined within the *Covert Surveillance and Property Interference Revised Code of Practice*.

5.2 **Duration**

5.2.1 DS authorisations will cease to have effect after 3 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., 3 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 12 months from the date of approval.

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

5.2.5 Urgent verbal authorisations are no longer permitted.

5.2.6 For CHIS authorisations, legal advice must be sought, particularly for those that involve the use of juveniles (for which the duration of such an authorisation is 4 months

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

5.3 **Review**

5.3.1 An Investigating Officer must carry out a regular review of authorisations, as frequently as is necessary and practicable, and 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 Monitoring Officer 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, and 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 and the RIPA Monitoring Officer.

5.4 **Renewals**

5.4.1 An Investigating Officer may ask for and an Authorising Officer can grant, subject to judicial approval, a renewal of an authorisation before it would cease to have effect.

An application for a renewal must not be made more than 7 days before the authorisation is due to expire.

5.4.2 A renewal may last for up to 3 months, effective from the date that the previous authorisation would cease to have effect.

5.4.3 An Authorising Officer may 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.

The original authorisation should be cancelled, and a new authorisation sought, granted by an Authorising Officer and approved by the Court.

5.4.5 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 'Monitoring Officer, or the Home Office website address given in **Appendix B**).

5.4.6 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 Monitoring Officer.

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 it should be cancelled as soon as the operation for which an authorisation was sought ceases to be necessary or proportionate.

This applies to both original applications and renewals (see forms '*Cancellation of Directed Surveillance*' and '*Cancellation of CHIS*' available from the RIPA Monitoring Officer, 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 Monitoring Officer.

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.

A '*relevant error*' means an error made by the Council when carrying out activity overseen by IPCO, the full definition of which may be found in

section 231(9) of the *Investigatory Powers Act 2016*.

5.6.2 If the error is of a serious nature then the Commissioner may require that the person concerned is informed of the error.

5.6.3 All relevant errors or queries in relation to potential errors must be brought to the attention of the RIPA Monitoring Officer at the first opportunity, who will report to IPCO where necessary.

5.7 **Review of Policy and Procedure**

5.7.1 The Audit Committee will receive annual reports on the use of RIPA.

5.7.2 The Audit Committee will approve and review the RIPA Policy, the use of RIPA, and RIPA powers on an annual basis and ensure compliance with the relevant Codes of Practice

5.7.3 This Policy is based on the requirements of RIPA and relevant Codes of Practice

5.7.4 The Council takes responsibility for ensuring that its RIPA procedures are continuously improved and asks that any Officers with suggestions contact the RIPA Monitoring Officer in the first instance.

6 The RIPA Monitoring Officer

6.1 The RIPA Monitoring Officer will:

6.1.1 provide a Unique Reference Number for each authorisation sought;

6.1.2 keep copies of the forms for a period of at least 3 years;

6.1.3 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;

6.1.4 provide administrative support and guidance on the processes involved;

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

6.1.6 monitor each department's compliance and act on any cases of non-compliance;

6.1.7 provide training and further guidance on and awareness of RIPA and the provisions of this Policy; and

6.1.8 review the contents of the Policy, in consultation with Investigating Officers, Authorising Officers and the Senior Responsible Officer.

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

6.3 All cancellations must be passed to the RIPA Monitoring Officer.

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

6.4.1 authorisations are only sought and given where appropriate;

6.4.2 authorisations are only sought and renewed where appropriate;

6.4.3 authorisations are reviewed regularly;

6.4.4 authorisations are cancelled where appropriate; and

6.4.5 they act in accordance with the provisions of RIPA.

7 Legal advice

Appropriately designated Officers within Legal Services (Regulation Team) will provide legal advice where necessary to Investigating Officers making, renewing or cancelling authorisations, including making applications for judicial approval. Please use the email address below to contact the Regulation Team.

regulation-prosecution@northumberland.gov.uk

8 Joint investigations/collaborative working

8.1 Where joint investigations are carried out with other agencies, such as the Department for Work and Pensions ('*DWP*') or the Police, the RIPA Monitoring Officer must 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.

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

8.3 Where possible, Public Authorities should seek 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.

9 National Anti-Fraud Network (in relation to interception of Communications Data specifically)

9.1 Local Authorities can now only access communications data via the National Anti-Fraud Network ('*NAFN*').

9.2 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, and which was created as a centre of excellence to provide data and intelligence to its members, including assisting members in the provision of effective corporate and financial governance.

9.3 NAFN maintains all data in a secure and confidential environment conforming to Government legislation and national best practice.

10 Online Covert Activity

10.1 The Council is aware in an increasing digital world and the growth of the

internet, there is a need to gather information that may only be available online. It is essential that that the Council, is able to access and obtain any relevant information so it can be used lawfully to fulfil statutory obligations. Investigating Officers should be aware that some information can be accessed without authorisation, however:

"*if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered."*[1]

10.2 Where an online investigation or any type of monitoring is to be conducted in a covert manner and is for a specific investigation and is likely to result in private information being obtained then an investigating officer should consider an authorisation.

10.3 Where an investigating officer is intending to engage with others online without disclosing their identity, then this may require a CHIS authorisation, before even considering this type of activity and authorisation, the officer should seek advice from an authorising officer.

10.4 It is accepted that some online platforms have a reduced or no expectation of privacy, such as the information which is in the public domain. This could include, for example information that is on an accessible database such as Companies House. There are also public social media sites and websites which publish information and communicate to a wide audience. However, investigating officers should always consider the nature of the site or platform, as it is possible that although the material is widely available, the intention of making that material available was not for it to be used in an investigation. If an investigating officer is concerned over the nature of site or platform and the question of privacy, they should seek advice from an authorising officer.

10.5 The current Code of Practice in relation to Covert Surveillance and Property inference covers online covert activity in detail, the following examples are taken from the Code and included here for ease of reference, although investigating officers should be familiar with the Code as whole.

Example 1:

A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2:

A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following

[1] CHIS Code (publishing.service.gov.uk)

paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

Example 3:

A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or 20 operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.[2]

11. Complaints

11.1 The Investigatory Powers Tribunal ('*IPT*') has jurisdiction to investigate and determine complaints against a Public Authority's use of investigatory powers, and is the only appropriate tribunal for human rights claims against the intelligence services.

11.2 All complaints for the use of powers should be directed to the IPT.

[2] CHIS Code (publishing.service.gov.uk)

Appendix A

Appointed Officers

The respective roles of Senior Responsible Officer, RIPA Monitoring Officer and Authorising Officers for the purposes of RIPA shall be assigned to the following posts within the Council.

This Appendix may be substituted from time to time should any job titles for any of the assigned posts change, or should the role be assigned to another qualifying post.

RIPA Officer role	**Assigned to the following posts:**
Senior Responsible Officer	Executive Director of Place and Regeneration
Authorising Officers (Directed Surveillance)	Chief Executive and Head of Paid Service Executive Director Adults, Ageing and Wellbeing Executive Director of Children, Young People and Education Head of Public Protection Public Health Protection Unit Manager Corporate Fraud Manager Chief Fire Officer
Authorising Officer (CHIS)	Chief Executive and Head of Paid Service Executive Director Adults, Ageing and Wellbeing Executive Director of Children, Young People and Education
RIPA Monitoring Officer	Director of Law & Corporate Governance / Monitoring Officer

This Appendix took effect January 2024

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 utilised in line with the Home Office 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:-

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

Directed Surveillance

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

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

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

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

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

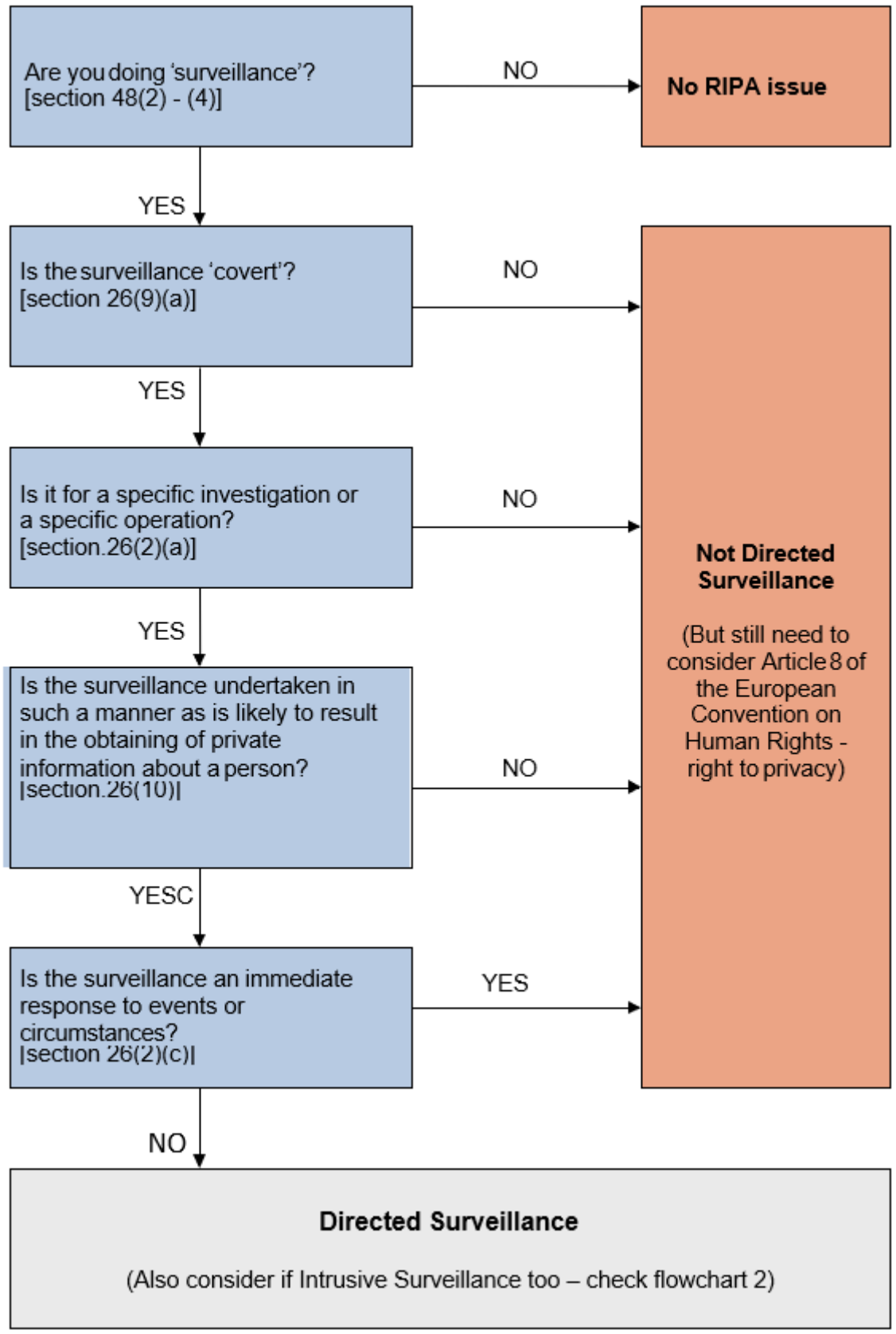
https://www.gov.uk/government/publications/cancellation-of-covert-human-intelligence- sources-chis

Appendix C

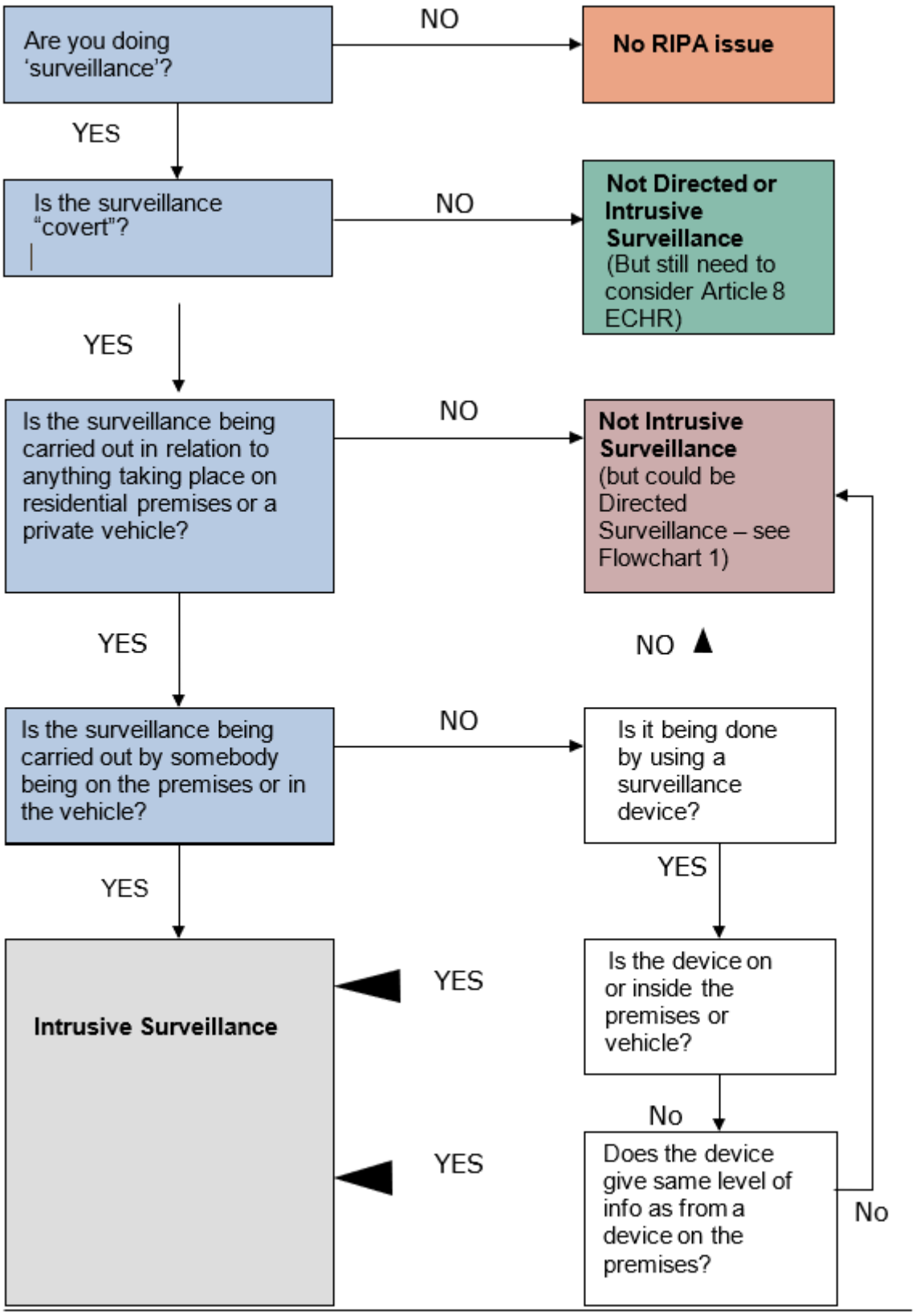
Flowcharts

Flowchart 1 – Are you carrying out Directed Surveillance?

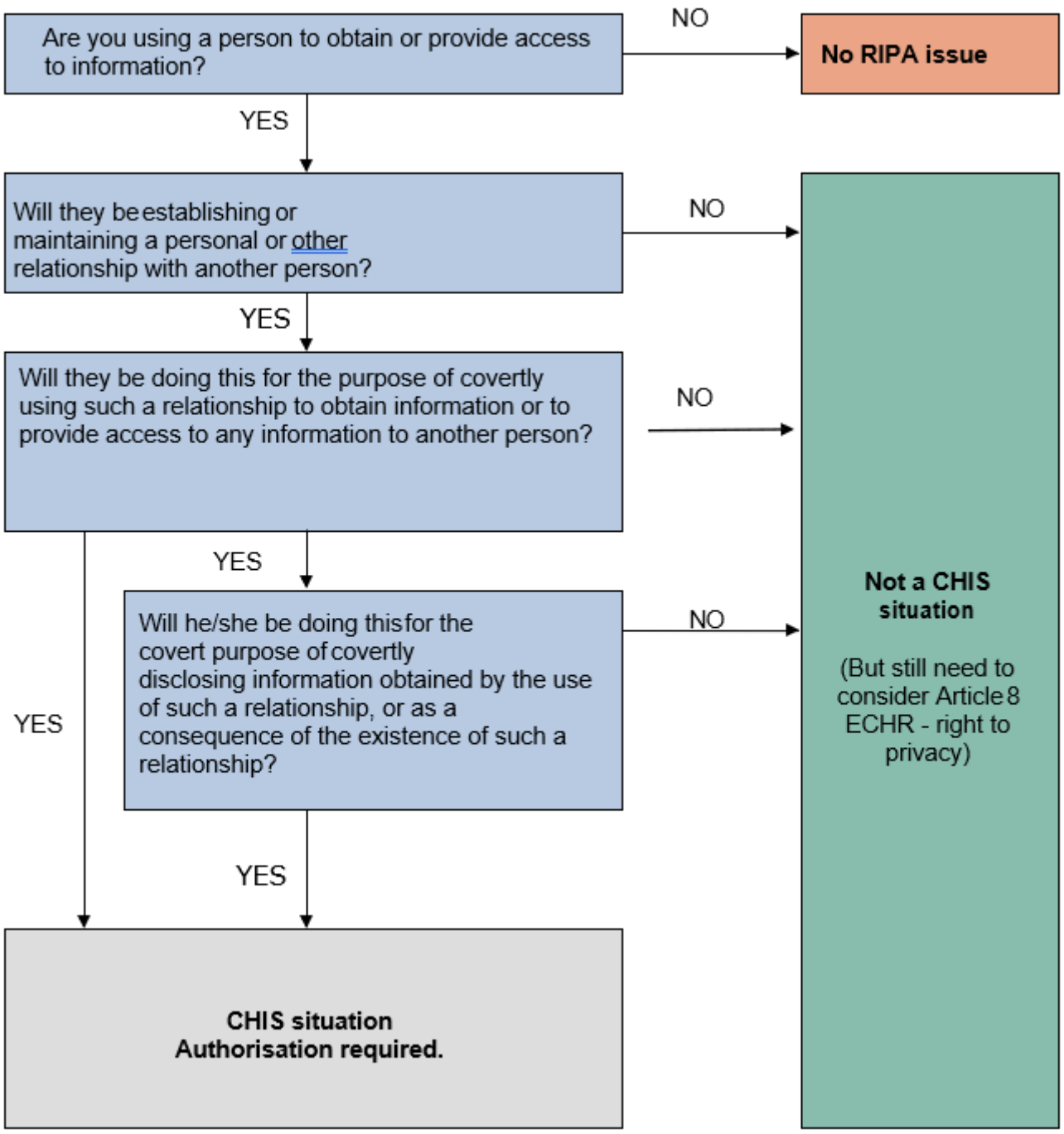
All references are to the relevant sections of RIPA.



Flowchart 2 – Are you carrying out Intrusive Surveillance?



Flowchart 3 - Are you using a CHIS? [section 26(8)]



Appendix D

Codes of Practice

https://www.gov.uk/government/publications/interception-of-communications- code-of-practice-2016

https://www.gov.uk/government/publications/equipment-interference-code-of-practice

https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition- and-disclosure-of-communications-data

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

https://www.gov.uk/government/publications/code-of-practice-for-investigation-of-protected-electronic-information