Public Document Pack

Supplementary Agenda

Contact Officer: Darius Zarazel, Democratic Services Officer
Tel: 07917 088376
E-mail: Darius.Zarazel@southandvale.gov.uk
Date: 8 April 2024
Website: www.southoxon.gov.uk www.whitehorsedc.gov.uk

A MEETING OF THE

Joint Audit and Governance Committee

WILL BE HELD ON MONDAY 15 APRIL 2024 AT 6.30 PM
MEETING ROOM 1, ABBEY HOUSE, ABBEY CLOSE, ABINGDON, OX14 3JE

To watch this virtual meeting, follow this link to the council's YouTube channel.

Members of the Committee:

South Oxfordshire District Council
Mocky Khan (Co-Chair)
Peter Dragonetti
Leigh Rawlins
Tony Worgan

Vale of White Horse District Council
Emily Smith (Co-Chair)
Oliver Forder
Judy Roberts
Andrew Skinner

Preferred Substitutes:

South Oxfordshire District Council
James Barlow
David Bretherton
Sam Casey-Rerhaye
Katharine Keats-Rohan
Axel Macdonald
Denise Macdonald
Jo Robb
David Turner

Vale of White Horse District Council
Andy Cooke
Eric de la Harpe
Jenny Hannaby
Mike Pighills

Alternative formats of this publication are available on request. These include large print, Braille, audio, email and easy read. For this or any other special requirements (such as access facilities) please contact the officer named on this agenda. Please give as much notice as possible before the meeting.

Vivien Williams
Head of Legal and Democratic (Interim)

8 Regulation of Investigatory Powers Act 2000 (RIPA) annual review (Pages 3 - 64)

To receive the report from the Head of Legal and Democratic (Interim).

The report will inform the Committee regarding the council's use of directed surveillance and covert human intelligence sources during 2022 and 2023 as required by the statutory code of practice in our enforcement work having proper regard to the principles of necessity, proportionality and lawfulness. It will also seek approval for revisions to the council's RIPA policy, procedures and action plan.

Recommendations:

That the committee:

a) notes that surveillance is one of the tools available to the councils as part of their law enforcement functions.

b) consider and note the council's use and compliance with RIPA.

c) approve the amendments made to the currently approved Regulation of Investigatory Powers Act 2000 Policy and Procedures, for use by council teams as part of their work.

d) agree the conclusions of this report and support the recommended actions in the action plan.

e) authorises the Head of Legal and Democratic (Interim) to make such changes to the Policy and Procedures documents as she may consider necessary from time to time to ensure ongoing compliance with the requirements of the 2000 Act and associated guidance.

Joint Audit and Governance Committee

South Oxfordshire District Council
Listening Learning Leading

Vale of White Horse District Council

Report of Head of Legal and Democratic (Interim)

Author: Pat Connell

Telephone 07717 274699

E-mail: pat.connell@southandvale.gov.uk

DATE: 15 April 2024

Regulation of Investigatory Powers Act 2000 (RIPA) annual review

Recommendation(s)

That the committee:

a) notes that surveillance is one of the tools available to the councils as part of their law enforcement functions.

b) consider and note the council's use and compliance with RIPA.

c) approve the amendments made to the currently approved Regulation of Investigatory Powers Act 2000 Policy and Procedures, for use by council teams as part of their work.

d) agree the conclusions of this report and support the recommended actions in the action plan.

e) authorises the Head of Legal and Democratic (Interim) to make such changes to the Policy and Procedures documents as she may consider necessary from time to time to ensure ongoing compliance with the requirements of the 2000 Act and associated guidance.

Implications (further detail within the report)	**Financial**	**Legal**	**Climate and Ecological**	**Equality and diversity**
	No	**Yes**	No	No
Signing off officer	**Simon Hewings**		**Heather Saunders**	**Abi Witting**

Purpose of Report

1. To inform the Committee regarding the council's use of directed surveillance and covert human intelligence sources during 2022 and 2023 as required by the statutory code of practice in our enforcement work having proper regard to the principles of necessity, proportionality and lawfulness. To also seek approval for revisions to the council's RIPA policy, procedures and action plan

Strategic Objectives

2. Managing and monitoring compliance with RIPA will support openness and transparency in South Oxfordshire District Council and working in an open and inclusive way in Vale of White Horse District Council.

3. Working to adopted and agreed RIPA policies and procedures will facilitate the use of covert surveillance as a legitimate and effective tool in enforcement investigations. It will also help ensure the lawfulness of such activity, thereby avoiding potentially costly and harmful legal challenges to our actions.

Background

4. The councils carry out a number of statutory functions that may require resort to enforcement action of many different types, and investigations carried out into breaches or suspected breaches of the law may lead the councils to take action in the courts, including criminal prosecutions. Protecting the environment from harm, particularly from illegal waste disposal (fly-tipping), fraud, licensing, planning and various aspects of health and safety are all areas of the councils' work where the councils and our residents are concerned to see effective enforcement action being taken against illegal activity. The ability to take such effective action may give rise to a need for investigative work, and the deployment of a range of techniques by the service teams who are charged with regulatory enforcement. Directed covert surveillance, and the use of covert human intelligence source (CHIS) are techniques that the councils may deploy in investigative work, and RIPA establishes a legislative framework within which the councils may seek to legitimately undertake such activity.

5. The 'law of RIPA', and the parameters of the legislation, are set out in a degree of detail in the attached documents, Regulation of Investigatory Powers Act 2000 Policy and Regulation of Investigatory Powers Act 2000 Procedures. The policy and procedures endorsed in 2020 by this committee have been reviewed and updated in accordance with current guidance and the Committee is asked to approve the amended updated documents. The detail that is included in those documents will therefore not be repeated in the body of this report. It may be helpful however for councillors to understand that RIPA does not of itself provide local authorities with powers to undertake covert surveillance that they otherwise might not have. What

RIPA and its associated guidance does do, is to establish a framework of principles against which the lawfulness of such surveillance activity might be able to be judged.

6. The Regulation of Investigatory Powers Act 2000 (RIPA) came into force in 2000 and governs the acquisition and disclosure of communications data and the use of covert surveillance by local authorities. This is supported by a set of codes of practice setting out processes and safeguards for a number of investigatory powers.

7. The councils can use powers under RIPA to support core functions for the purpose of prevention and detection of crime where an offence may be punishable by a custodial sentence of 6 months or more or are related to the underage sale of alcohol and tobacco. There are three processes available to local authorities under RIPA,
    - Directed Surveillance,
    - Covert Human Intelligence Sources (CHIS), and
    - the acquisition and disclosure of communications data.

8. RIPA and Codes of Practice set out the procedures that local authorities must follow when undertaking surveillance. For example, approval by Authorised Council Officers for Directed Surveillance / CHIS applications to show that the proposed use of the powers is “necessary and proportionate”.

9. The councils are required to have a Senior Responsible Officer to maintain oversight of the RIPA arrangements, procedures and operations. The councils’ Monitoring Officer performs this function and is responsible for the integrity of the process for managing the requirements under RIPA.

10. The Investigatory Powers Commissioner’s Office (IPCO) provides independent oversight of the use of investigatory powers by public authorities as outlined in the Investigatory Powers Act 2016 (IPA). In 2019, Part 3 of the IPA was introduced which amended the acquisition of communications data and overhauled the way these powers are authorised and overseen. The IPA has introduced the Office for Communications Data Authorisation (OCDA) which is now responsible for independently authorising all applications for communications data. This has removed the requirement for local authorities to seek judicial approval for communications data. In addition, the legislation has broadened the range of communications data available including access to location data.

11. The acquisition of communications data is undertaken through the National Antifraud Network (NAFN). They act as the single point of contact for many local authorities and ensure any application is RIPA/ IPA compliant. It is NAFN that are audited by the commissioners.

Annual usage of investigatory powers

12. The Home Office Code for Covert Surveillance and Property Interference recommends that councillors, whilst by law are not permitted to be involved in making decisions or specific authorisations for the local authority to use its powers under Part II of the Act, should review the councils’ use of the legislation at least annually and provide approval to its policies.

13. The IPCO are required by law to gather statistical data from public authorities on their use of investigatory powers under the relevant legislation. Annual returns are submitted to the IPCO by the end of each January covering the previous calendar year.

14. For the period 1 January 2022 to 31 December 2022 and for 1 January 2023 to 31 December 2023 the statistical returns for both South Oxfordshire District Council and Vale of White Horse District Council was that no applications or authorisations had been made for either directed surveillance or covert human intelligence sources. There were no reported incidents of the councils having misused powers under RIPA during this period.

15. No applications for the disclosure of communications data were made during the period 1 January 2022 to 31 December 2022 or during the period 1 January 2023 to 31 December 2023.

Inspection outcomes

16. IPCO inspections of local authorities are normally every three years, and the councils were last subject to a remote inspection by the IPCO during 2021. As summarised in the commissioner's letter of 31 March 2021 to our Chef Executive, the IPCO noted that both councils are limited users of the surveillance powers but demonstrated the importance of maintaining strong policies and procedures in an effort to ensure a good level of compliance.

17. The 2021 inspection noted that the actions from the January 2018 review had been discharged and raised new recommendations which were added to an action plan in May 2021.

Action plan

18. The current action plan updates actions brought forward from previous years and additional actions identified since.

Policy changes

19. The RIPA policy and procedures documents have been reviewed and updated to include items identified within the 2021 inspection letter and guidance provided by the IPCO within newsletters.

Financial Implications

20. There are no financial implications attached to this report.

Legal Implications

21. Each Council has demonstrated compliance with its statutory obligations under RIPA to the satisfaction of the Surveillance Commissioner following inspection in January 2021 and continues to update its policy and provide training for officers.

22. This report to members complies with the Code of Practice requirement that members should be updated annually on RIPA activity and endorse the Policy, including any changes to it, for the coming year.

Climate and ecological impact implications

23. There are no direct climate or ecological implications arising from this report.

Equalities implications

24. This report is for information only and therefore there are no equalities implications.

Risks

25. The Councils are required to comply with the statutory provisions and guidance governing the RIPA regime and any recommendation made by the Inspector on behalf of the Commissioner. Officers need to be aware of the RIPA powers so that there is no risk of surveillance or CHIS activity being undertaken without the correct oversight and approvals being in place. Adherence to a robust RIPA policy and procedures will help avoid legal challenges to the lawfulness of the councils' actions which would be likely to be costly and could potentially cause reputational harm.

Other Implications

26. The councils continue to operate a system of closed-circuit television (CCTV) across six market towns in the districts. There are 86 cameras in total, monitored from a control room within Abingdon Police Station, by staff employed by the councils. The management, operation and use of this system is undertaken in accordance with a code of practice and an operational handbook separate from the policy and procedures document accompanying this report, it being noted that CCTV of public place activity generally is considered to be classed as overt rather than covert activity.

27. In a similar vein, the presence of cameras which are deployed to detect and prevent the crime of fly tipping at 'hotspot locations' in the districts is normally accompanied by signage placed nearby, informing the public that surveillance takes place. This means that the process of surveillance is not strictly subject to the requirements of 'full RIPA', as the surveillance is overt. The carrying out of this kind of surveillance activity however is still subject to a process of assessment based on principles of necessity and proportionality, and consideration of rights of privacy.

28. Officers in the waste team use Body Video cameras on occasion. The management operation and use of such cameras is undertaken in accordance with documented guidance and generally falls to be considered as overt rather than covert activity.

Conclusion

29. The adoption of the updated policy and procedures documents setting out the way in which the councils may seek to use covert surveillance as a tool in investigative work will facilitate effective enforcement work and will help ensure that the councils operate within the legal rules that regulate such activity. The committee is therefore asked to endorse the updated documents attached to this report, Regulation of Investigatory Powers Act 2000 Policy and Procedures, for adoption and use within the councils and to authorise the Head of Legal and Democratic to make further changes to keep the document up to date as appropriate.

Background Papers

- RIPA Policy
- RIPA Procedure
- RIPA Action Plan

Regulation of Investigatory Powers Act 2000 (RIPA) Policy

South Oxfordshire and Vale of White Horse District Council

South Oxfordshire District Council
Listening Learning Leading

Vale of White Horse District Council

Change Record

Change Record	
Policy Title	Regulation of Investigatory Powers Act 2000 (RIPA) Policy
Version Number	V1
Owner(s)	Pat Connell
Author(s)	Pat Connell
Approved by	
Effective date	
Renewal date	

Table of Contents

1 Introduction

1.1 Purpose

1.1.1 This policy is the framework on which the councils apply the provisions of The Regulation of Investigatory Powers Act 2000 (RIPA) as it relates to covert surveillance. It must be read in conjunction with the statutory codes of practice issued by the Secretary of State and any additional guidance provided by Investigatory Powers Commissioner's Office (IPCO). This policy is supported by a RIPA Procedure which sets out a guide to practice, responsibilities and procedure to be followed.

1.1.2 All references to the Home Office Codes of Practice relate to the latest versions which were issued in relation to covert surveillance and covert human intelligence sources, and in relation to the acquisition and disclosure of Communications Data. References to the Code of Practice and other relevant Guidance document relate to the latest version which was issued.

1.1.3 The Regulation of Investigatory Powers Act 2000 (RIPA) is the domestic law that regulates the way law enforcement agencies, and public bodies conduct surveillance for the purposes of law enforcement. The fundamental requirement of RIPA is that when the councils consider undertaking directed surveillance or using a covert human intelligence source (CHIS) it must only do so if the activity has been authorised by an officer with appropriate powers, and the relevant criteria are satisfied.

1.2 Scope

1.2.1 This policy applies to all staff and agents working for the councils. Although the councils may have limited use of the powers under RIPA, it is important that there is good awareness and knowledge across service teams so that we do not inadvertently use any approach that may contravene RIPA.

1.2.2 As the councils have a number of functions to undertake which involve the enforcement of laws and regulations, for example, environmental protection, health and safety, licensing, fraud investigation and planning enforcement, officers will need to conduct investigations and where appropriate take legal proceedings. The councils will not normally make use of covert surveillance and similar activities unless it is necessary for an investigation.

1.2.3 All investigations or enforcement actions involving covert surveillance, or the use of a CHIS must comply with the provisions of RIPA.

2 Use of RIPA vs Human Rights

2.1.1 The Human Rights Act 2000 (HRA) requires the councils to have respect for the private and family life of citizens. However, in rare cases, it may be lawful, necessary and proportionate for the councils to act covertly in ways that may interfere with an individual's rights.

2.1.2 The rights conferred by Article 8 of the HRA are qualified, so it is still possible for a public authority to infringe those rights providing it is necessary and proportionate.

2.1.3 **It is necessary:** Necessity means that in the particular circumstances of each enquiry there is no reasonably available overt method of obtaining the information that is being sought. This test will have to be applied to each case on its own merits but if there is a reasonable alternative to covert surveillance then the necessity test will probably not be satisfied.

2.1.4 **It is proportionate:** Judging proportionality will probably involve three considerations:

- Is the proposed method of surveillance excessive in relation to the seriousness of the matter that is being investigated? Is it proportional to the mischief under investigation?
- Is there a reasonable available alternative method of investigation that would be less intrusive of privacy rights? i.e. It is the only option, other overt means having been considered and discounted.
- Can collateral intrusion be avoided, and is the surveillance proportional to the degree of anticipated intrusion on the target and others? In addition to the subject there may be a possibility that the privacy rights of a third party may be infringed during surveillance.

2.1.5 By the application of authorisation procedures and Magistrates Court approval, RIPA ensures that a balance is maintained between the public interest and the human rights of individuals.

3 The Investigatory Powers Commissioner's Office (IPCO)

3.1 Role of the IPCO

3.1.1 The IPCO is overseen by the Investigatory Powers Commissioner (IPC) and supports the IPC and Judicial Commissioners in fulfilling their duties under the Investigatory Powers Act 2016. The IPCO is an Arm's Length Body of the Home Office and acts independently of the Government.

3.1.2 The IPC has responsibility for reviewing the use of investigatory powers by public authorities. This includes independent review of applications from public authorities to use the most intrusive investigatory powers and check compliance with the law.

3.1.3 The IPCO has a statutory obligation to inspect the use of investigatory powers by public authorities. Inspections will involve either an in person visit or remote access to records to scrutinise the records of any use of RIPA. As well as authorisation records and supporting documents, the review can include examining training materials and our governance structures.

3.2 Requests for IPCO inspection reports

3.2.1 The IPCO itself is not covered by the Freedom of Information Act 2000 (FOIA) and if councils receive requests for disclosure of IPCO inspection report we must respond as if the reports are our own documents.

3.2.2 Before making any disclosure, the receipt of the request should be brought to the attention of the IPCO's Data Protection Officer via info@ipco.org.uk who should be consulted with about the release.

4 Impact of not following RIPA

4.1.1 It is possible that unauthorised surveillance will be a breach of a person's right to privacy under HRA Article 8. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not obtained, the surveillance carried out will not have the protection that RIPA affords.

4.1.2 If the correct procedures are not followed:

- the authorisation will not take effect as it will not be approved by the Magistrates Court if there are not reasonable grounds.
- Court proceedings that rely upon the information obtained by surveillance may be undermined.
- a complaint of maladministration may be made to the Ombudsman.
- the councils could be the subject of an adverse report by the Investigatory Powers Commissioner's Office
- a claim could be made leading to the payment of compensation by the councils.

5 Use of RIPA

5.1.1 RIPA does not;

- Make unlawful anything that is otherwise lawful.
- Impose any new statutory duties (N.B. but see paragraphs 1.5 –1.7 on the possible consequences of non-compliance)
- Prejudice or disapply any existing powers available to the councils to obtain information by any means not involving conduct that is governed by RIPA. (For example, it does not affect the councils' current powers to obtain information from the DVLA or the Land Registry).

5.1.2 If the RIPA procedures are followed correctly the conduct of an investigation will be deemed lawful for all purposes (section 27 RIPA). This protection extends to criminal and civil proceedings, and a complaint to either the Local Government Ombudsman or the Investigatory Powers Tribunal. It therefore provides protection both for the councils and any officer who may have been involved in an investigation.

5.1.3 Applications to the Magistrates' Court for approval of an authorisation must be made in accordance with the requirements of the Court.

5.1.4 The use of the powers conferred by RIPA is subject to scrutiny by the Investigatory Powers Commissioner's Office, which carries out periodic inspections of the councils' practices and procedures. Furthermore, RIPA also provides for the establishment of a Tribunal to determine complaints about the use of RIPA powers. It is therefore essential that surveillance is always carried out in compliance with RIPA, the policies and codes of practice referred to in this document and any advice or guidance that may be issued from time to time by the Head of Legal and Democratic

5.1.5 RIPA provides a means of authorising certain acts of covert surveillance for a variety of purposes. To fully understand the effects of RIPA, it is essential to understand the various types of activity that are covered, and those that are not permitted, and the purposes that will justify surveillance.

5.2 Provisions of RIPA that apply to the councils

5.2.1 The provisions of RIPA that apply to Local Authorities provide a regulatory framework that permits;

- The use of Directed Surveillance (Part 3)
- The Use of Covert Human Intelligence Sources (Part 4)
- The Acquisition and Disclosure of Communications Data (Part 5)

6 Types of Surveillance

6.1.1 Local Authorities and the Police are permitted under RIPA to carry out covert directed surveillance and to use covert human intelligence sources the definitions for each being as follows.

6.1.2 "Surveillance" includes:

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations or their other activities or communications.
- recording anything monitored, observed or listened to in the course of surveillance.
- Surveillance by, or with, the assistance of a surveillance device, which will include cameras, video, and listening or recording devices.

6.1.3 Surveillance can be either **overt** or **covert**.

6.2 Overt Surveillance (outside of RIPA)

6.2.1 Most of the surveillance undertaken by the councils will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases officers will be going about councils' business openly (e.g., a routine inspection by an Environmental Health Officer) or will have notified the subject of the investigation that they are likely to be under surveillance. In the latter case officers need to be particularly alert to the possibility that the proposed surveillance may entail collateral intrusion into the lives and activities of persons other than the subject of the investigation (e.g., a visitor to premises). If there is the slightest possibility of collateral intrusion a RIPA authorisation should be obtained before any surveillance is carried out.

6.2.2 Surveillance will be overt if the subject has been told it will happen. This will be the case where a noisemaker is warned that recordings will be made if the noise continues; or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or without identifying themselves to the owner/proprietor to check that the conditions are being met. Such warnings should be given to the person concerned in writing.

6.2.3 Overt surveillance does not require any authorisation under RIPA. Neither does low-level surveillance consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the RIPA Monitoring Officer or the Senior Responsible Officer.

6.2.4 Home Office guidance also suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement officers as part of general observation does not need to be regulated by RIPA, if the systematic surveillance of an individual is not involved. However, if binoculars or cameras are used in relation to anything taking place on any residential premises, or in any private vehicle, the surveillance can be intrusive even if the use is only fleeting. Any such surveillance will be intrusive "if it consistently provides information of the same quality as might be expected to be obtained from a device actually present on the premises or in the vehicle". The quality of the image obtained rather than the duration of the observation is what is determinative. It should be remembered that the councils are not permitted to undertake intrusive surveillance.

6.2.5 Use of body worn cameras should be overt. Badges should be worn by officers stating body cameras are in use and it should be announced that recording is taking place. In addition, cameras should only be switched on when recording is necessary – for example, when issuing parking tickets.

6.3 Use of Covert Surveillance

6.3.1 Covert surveillance is covert where it is 'carried out in a manner **calculated** to ensure that the person or persons subject to the surveillance are unaware that it is or may be taking place'.

6.3.2 RIPA requires the authorisation of two types of covert surveillance (directed surveillance and intrusive surveillance) plus the use of covert human intelligence sources (CHIS) or acquisition of Communications Data.

6.4 Covert Human Intelligence Source (CHIS)

6.4.1 A person is a covert human intelligence source if that person 'establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information or providing access to any information to another person, or they covertly disclose information obtained by the use of such a relationship'. Covert in this context means that it is calculated that the subject should be unaware of the purpose of the relationship.

6.4.2 A member of the public who volunteers information to the councils is not a covert human intelligence source.

6.4.3 The conduct or use of CHIS must be authorised in accordance with RIPA.

- **Conduct** of a CHIS. This is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining or passing on information.
- **Use** of a CHIS. This includes inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

6.4.4 The use of a juvenile CHIS may only be authorised for four months at a time.

6.4.5 If a CHIS authorisation includes a source that is a vulnerable person or a juvenile, then the Investigatory Powers Commissioner (IPC) must be informed within seven days of the authorisation. These types of authorisations will be kept under close review by the IPC.

6.4.6 Members of the public who report allegations of anti-social behaviour and are asked to keep a note of incidents will not normally be CHIS as they are not usually required to establish or maintain a covert relationship.

6.4.7 **Noise -** Persons who complain about excessive noise, and are asked to keep a noise diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g., the decibel level) will not normally capture private information (if non-verbal noise such as music, machinery or an alarm), and therefore does not require authorisation. Recording sound with a DAT recorder or similar, could constitute covert surveillance, although if it can be heard from the street outside, may (as per the Code of Practice) be regarded as having forfeited any claim to privacy. The easiest option is for this to be undertaken overtly – for example it will be possible to record sound if the noisemaker is warned that this will occur if the level of noise continues.

6.4.8 **Test Purchases.** Carrying out test purchases will not normally require the purchaser to establish a relationship with the supplier with the covert 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). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product e.g., illegally imported wild meat, or using covert recording equipment is likely to require authorisation as a CHIS. Similarly, using hidden recording devices to record what is going on in the shop (e.g., a hidden CCTV Camera) may require authorisation as directed surveillance. A combined authorisation can be provided if a CHIS is carrying out directed surveillance.

6.4.9 Note 251 of the OSC's 2016 Procedures & Guidance document states:
251. A local authority may prefer to seek the assistance of the police or another public authority to manage its CHIS. In such a case a written protocol between the parties should be produced in order to ensure that an identified CHIS is properly managed (see CHIS Code of Practice 6.12). In the absence of such an agreement the local authority must be capable of fulfilling its statutory responsibilities.

6.5 Directed surveillance.

6.5.1 Directed Surveillance is surveillance that is:

- covert but not intrusive surveillance
- undertaken for the purpose of a specific investigation or operation carried out in such a manner as is likely to result in the obtaining of private information about a person (whether one specifically identified for the purposes of the investigation or operation)

- not carried out as an immediate response to events which would otherwise make seeking authorisation under RIPA unreasonable (e.g., spotting something suspicious and continuing to observe it)

6.5.2 Surveillance by way of an immediate response to events or circumstances where it would not be 'reasonably practicable' for an authorisation to be sought is not included within the provisions of RIPA.

6.6 Examples of types of surveillance

Type of surveillance	Examples
Overt	• Signposted Town Centre CCTV cameras (in normal use) • Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. • Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert, but not requiring prior authorisation	• CCTV cameras providing general traffic, crime or public safety information. • Viewing of publicly available social media profile and postings. (Use of Human Rights Act assessment needed)
Directed, **MUST be RIPA** authorised	• Covert CCTV cameras at a fly-tipping hotspot • Covert and targeted following of a benefit claimant who is suspected of failing to declare earnings from a job, can be by investigators/observation, CCTV or social media
Intrusive or interfering with private property – **WE CANNOT DO THIS!**	• Planting a listening or other electronic device (bug) or camera in a person's home or in / on their private vehicle or on their person. • Surveillance of a place used for legal consultations

7 Private Information.

7.1.1 This phrase is defined in RIPA section 26(10) as including any information relating to a person's private or family life. The European Court of Human Rights has considered this definition and has found that private life is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by HRA Article 8. The Article also protects a right to identity and personal development and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is therefore a zone of interaction of a person with others even in a public context, which may fall within the scope of "private life".

7.1.2 The fact that covert surveillance occurs in a public place or on business premises does not necessarily mean that it cannot result in the acquisition of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about them and others that they come into contact with or with whom they associate. Similarly, although the overt use of CCTV cameras does not normally require authorisation, if the camera is used for a particular purpose that involves the prolonged surveillance of a particular person, a RIPA authorisation will be required.

8 EXCLUSIONS – Where we cannot use surveillance.

8.1.1 There are some instances where surveillance is not permissible in any circumstances.

8.2 Intrusive Surveillance.

8.2.1 RIPA provides that the councils **cannot** authorise intrusive surveillance. This is covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle, whether by way of a person or device.

8.2.2 It will also be intrusive surveillance where a device placed outside consistently provides information of the same or equivalent quality and detail, as might be expected if it were in the premises or vehicle.

8.2.3 Residential premises are any part of premises occupied for residential purposes or living accommodation, including hotel rooms or prison cells. However, it does not include common areas in blocks of flats and similar premises.

8.2.4 Private vehicle is a vehicle used primarily for private purposes by the owner or person entitled to use it.

8.2.5 Only the police or other law enforcement agencies are permitted to employ intrusive surveillance. Likewise, the councils have no statutory powers to interfere with private property.

8.3 Use of Children to gather information about parent/ guardian.

8.3.1 Authorisation may not be granted for the conduct or use of a source under the age of sixteen where it is intended that the purpose is to obtain information about their parent or any person who has parental responsibility for them.

8.3.2 Should there be an exceptional case where children are to be used as a CHIS, and this is not for the use described above, authorisation must at a specified level and for Local Authorities this is the Head of Paid Service.

8.4 Vulnerable Individuals

8.4.1 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 themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an individual may be vulnerable, they will only be authorised as a CHIS in the most exceptional of circumstances.

8.4.2 The use of a vulnerable individual as a CHIS requires authorisation at a specified level and for Local Authorities this is the Head of Paid Service.

9 Grounds for surveillance

9.1.1 Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a custodial sentence of a maximum term of at least 6 months' imprisonment, or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

9.1.2 Even if the person granting the authorisation believes that the authorisation is necessary, they must also be satisfied that the authorised activity is proportionate to what is sought to be achieved by it. This requires the Authorising Officer to balance the need for surveillance with the level of intrusion into any person's privacy.

9.1.3 Consideration should be given to collateral intrusion, which is interference with the privacy of persons other than the subject(s) of the surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

9.1.4 Confidential information. Careful consideration is also needed when there is a risk of obtaining confidential information. The Covert Surveillance and Property Interference defines this as:

"information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above 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 any legal obligation of confidentiality. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records".

9.1.5 In cases where it is likely that confidential information will be acquired the authorisation must be granted by the by the Head of the Paid4 Service (or in their absence by an authorised Head of Service).

9.1.6 An application for an authorisation must include a full assessment of the risk of any collateral intrusion or interference so that the Authorising Officer can consider this.

9.1.7 Authorising Officers must always consider the need for surveillance or CHIS and balance this against an individual's right to privacy under the Human Rights Act 1998. An officer seeking an authorisation should always be able to justify why it is necessary and why other, less intrusive, forms of investigation are unsuitable or have previously been tried without success and thus the matter has escalated to the requirement for covert surveillance.

10 Communications data - acquisition and disclosure of

10.1.1 The Investigatory Powers Act 2016 ('IPA') provided an updated framework for lawful acquisition of Communications Data, include the who, where, what, when and how a Local Authority can obtain communications and Communications Data.

10.1.2 The IPA sets out the three powers, under sections 60A, 61 and 61A, which can be used to authorise the acquisition of Communications Data (CD), dependent on the statutory purpose and urgency. Only section 60A is relevant to local authorities, although a number of new offences would also apply in terms of unlawful acquisition and disclosure of Communications Data.

10.1.3 Public Authorities can only apply if this is for 'the applicable crime purpose'. This means the data has to be wholly or partly Events data, the purpose of preventing or detecting serious crime; or in any other case, the purpose of preventing or detecting crime or of preventing disorder.

10.1.4 The types of Communications Data that Local Authorities' can access are Entity and Events Data, which are defined as:

- **Entity Data**: means any data which is about —
  (a) (i) an entity, (ii) an association between a telecommunications service and an entity, or (iii) an association between any part of a telecommunication system and an entity,

  (b) consists of or includes data which identifies or describes the entity (whether or not by reference to the entity's location) and is not events data.

- **Events Data:** any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time. Where the purpose of the acquisition is to prevent or detect crime, and the data required is events data, the offence or conduct of the offence being investigated must meet at least one of the definitions of serious crime.

10.1.5 The IPA has also removed the necessity for local authorities to seek Magistrates or Justice of the Peace approval to acquire Communications Data. All such applications must now be processed through the National Anti- Fraud Network (NAFN), who will consider the application prior to submitting this for approval to the Office for Communications Data Authorisations ('OCDA').

10.1.6 All applications must be approved before Communications Data is acquired. The Investigatory Powers Commissioner oversees the use of the powers (who with Judicial Commissioners have a role to approve authorisations to identify or confirm the identity of a journalist's source). The application process has otherwise been made more efficient through the ability to submit these electronically.

10.1.7 Sections 37 to 44 of the Police, Crime, Sentencing & Courts Act 2022 (PCSCA) came into force on 8 November 2022. This provides public authorities with a further power to extract data held on electronic devices.

10.1.8 Before action is taken, there must be a reasonable belief that information stored on the device will be relevant for one of three scenarios and satisfaction that the extraction of the information is necessary and proportionate to achieve the purpose.

10.1.9 The three scenarios provided under s37(2) are for the purpose of:

a) preventing, detecting, investigating or prosecuting crime;

b) helping to locate a missing person; or

c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.

10.1.10 To ensure any extraction of stored communication under s.37 remains lawful, it is essential that the criteria and procedures set out within the PCSCA and the association Code of Practice are fulfilled.

10.1.11 A failure to follow these procedures correctly could result in a s.3 IPA offence (unlawful interception) being committed.

11 RIPA and contracted service providers

11.1.1 It is important to note that the legislation does not only affect directly employed council staff. Where external agencies are working for the councils, carrying out the councils' statutory functions, the councils remain liable for compliance with its duties. It is essential that all external agencies comply with the regulations, as they are contractually obliged to do so. Therefore, work carried out by agencies on the councils' behalf should be properly authorised by one of the councils' designated Authorising Officers and requires Magistrates Court approval for applications and renewals. Authorisation for surveillance should not be sought on behalf of another statutory or other organisation or agency. The advice of the Senior Responsible Officer ('SRO') should be sought in the event of uncertainty.

12 Authorisations and roles

12.1 Authorisations in general

12.1.1 Authorisations may only be given by the Authorising Officers listed in the councils' RIPA procedures. Only the Head of Paid Service can authorise the use of a CHIS for a vulnerable person or juvenile or the acquisition of confidential information.

12.1.2 Applications for the acquisition of Communications Data can only be issued by a Home Office accredited single point of contact (SPoC). The National Anti-Fraud Network (NAFN) provides a SPoC service to local authorities.

12.1.3 Local authorities using the NAFN SPoC service will still be responsible for scrutinising the application for Communications Data prior to contacting NAFN.

12.1.4 The applicant officer must complete application forms in their entirety.

12.1.5 Authorisation under RIPA is quite separate from delegated authority to act under the councils' Scheme of Delegation. **RIPA authorisations are for specific investigations only and must be cancelled or renewed once the specific surveillance is complete, or about to expire.**

12.1.6 The Authorising Officer should not just "sign off" an authorisation, they must give **personal consideration** to the necessity and proportionality of the proposed action prior to applying to the Magistrates Court for approval and must personally ensure that the surveillance is reviewed and cancelled.

12.1.7 Any rejected applications must be entered into the RIPA log held by the RIPA Coordinating Officer.

12.2 Applications for directed surveillance.

12.2.1 In the case of applications for authority to carry out **directed surveillance** the Authorising Officer should:

- consider the relevant Codes of Practice
- consider whether the specific operation or investigation has been adequately described.
- be satisfied as to the reasons for the application.
- be satisfied that the directed surveillance is **necessary** in the circumstances of the particular case.
- be satisfied that the surveillance is **proportionate** to the stated purpose and objectives.
- be satisfied that the possibility of collateral intrusion has been avoided or minimised.
- consider the likelihood of confidential information being acquired.
- check that an appropriate review period has been listed on the application form.

12.2.2 **If there is an alternative practicable means of carrying out the surveillance, which is less intrusive, then the surveillance is neither necessary nor proportionate and should not be authorised. The least intrusive method should be used.**

12.3 Additional factors for authorising CHIS

12.3.1 In addition to considerations 12.2 above, when authorising the conduct or use of a CHIS the Authorising Officer must:

- be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved.
- be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS.
- consider the likely degree of intrusion of all those potentially affected.
- consider any adverse impact on community confidence that may result from the use or conduct, or the information obtained.
- ensure **records** contain statutory particulars and are not available except on a need-to-know basis.
- ensure that authorisations relating to the use of a juvenile CHIS are only for four months at a time.
- be satisfied that a full risk assessment has been undertaken.

12.4 The role of Senior Responsible Officer (SRO)

12.4.1 The councils' SRO is the Head of Legal and Democratic. The SRO is responsible for:

- the integrity of the process in place within the public authority for the management of CHIS and Directed Surveillance
- compliance with Part 2 of the Act and with the Codes
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
- engagement with the IPCO inspectors when they conduct their inspections, where applicable
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

12.5 The role of RIPA Coordinating Officer

12.5.1 The councils' RIPA Coordinating Officer is the Deputy Head of Legal (Operational) who is responsible for:

- dealing with the CHIS on behalf of the councils
  - directing the day-to-day activities of the CHIS
  - recording the information supplied by the CHIS
  - monitoring the CHIS's security and welfare.

13 Policy review

13.1.1 This policy will be kept under review and updates on at least an annual basis and will be presented to the Joint Audit and Governance Committee annually for approval.

Regulation of Investigatory Powers Act 2000 (RIPA) Procedures

South Oxfordshire and Vale of White Horse District Council

Change Record

Change Record	
Procedures Title	Regulation of Investigatory Powers Act 2000 (RIPA) Procedures
Version Number	V1
Owner(s)	Pat Connell
Author(s)	Pat Connell
Approved by	
Effective date	
Renewal date	

Table of Contents

1 Introduction

1.1 Purpose

1.1.1 These procedures set out a guide to practice for how the councils manage and record decisions relating to the provisions of The Regulation of Investigatory Powers Act 2000 (RIPA) as it relates to covert surveillance. This must be read in conjunction with the councils' RIPA Policy and statutory codes of practice issued by the Secretary of State and any additional guidance provided by Investigatory Powers Commissioner's Office (IPCO).

1.1.2 All references to the Home Office Codes of Practice relate to the latest versions which were issued in relation to covert surveillance and covert human intelligence sources, and in relation to the acquisition and disclosure of Communications Data. References to the Code of Practice and other relevant Guidance document relate to the latest version which was issued.

1.2 Scope

1.2.1 This procedure applies to all staff and agents working for the councils. Although the councils may have limited use of the powers under RIPA, it is important that there is good awareness and knowledge across service teams so that we do not inadvertently use any approach that may contravene RIPA.

1.3 Background

1.3.1 The main purpose of the Regulation of Investigatory Powers Act 2000 ("the Act") is to ensure that public bodies use their investigatory powers in accordance with the Human Rights Act 1998.

1.3.2 The investigatory powers covered by the legislation are:

(a) intrusive surveillance (on resident premises/in private vehicles) (**NB: The councils are not permitted to engage in intrusive surveillance)**

(b) covert surveillance in the course of specific operations

(c) the use of covert human intelligence sources (agents, informants, undercover officers)

1.3.3 For each of these powers the Act ensures that the law clearly covers the purposes for which they may be used, which authorities can use the powers, who should authorise each use of power, the use that can be made of the material gained, independent judicial oversight and a means of redress for any individual aggrieved by use of the powers.

1.3.4 All investigations or enforcement actions involving covert surveillance or the use of a CHIS must comply with the provisions of RIPA. The consequence of not obtaining an authorisation and approval under the Act may be that the action is in breach of the Human Rights Act and that any evidence so gained could be excluded in any proceedings that arise.

1.4 Some definitions

1.4.1 **"Covert"** Concealed, done secretly.

1.4.2 **"Covert surveillance"** Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

1.4.3 **"Directed surveillance**" Surveillance, which is covert, but not intrusive, and is undertaken for the purposes of a specific investigation or specific operation, 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 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 under Part II of the Act to be sought for the carrying out of the surveillance.

1.4.4 **"Intrusive surveillance"** Is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

1.4.5 **"Private information"** Includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

1.4.6 **"Confidential Information"** Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material.

2 Decisions register, records, retention and destruction

2.1.1 The register and all associated documents relating to authorisations and approvals, reviews, cancellations, or renewals and refused applications should be retained in an auditable format, with each particular authorisation and approval allocated a unique reference number cross referenced to a unique reference number for that particular investigation or activity.

2.2 Decisions register

2.2.1 A central register of RIPA authorisations will be maintained by the council's Head of Legal and Democratic, who is the council's Senior Responsible Officer for the purpose of ensuring the integrity of the council's RIPA processes under the Act, and statutory guidance issued in pursuance of the Act.

2.2.2 Day to day maintenance of the register and advice relating to RIPA issues is undertaken under the supervision of the Senior Responsible Officer by the council's Deputy Head of Legal (Operational), in the role of RIPA Coordinating Officer.

2.2.3 All officers should ensure that original signed documents are given to the RIPA Coordinating Officer (or in case of absence to another lawyer in the legal services team) upon issue in order to keep this register up to date. On receipt of a document to be included within the register, a date for review will be diarised.

2.3 Records

2.3.1 Records should be retained for a period of at least three years from the ending of the authorisation and should contain information as specified in the Code of Practice

2.4 Retention and destruction of results of investigations

2.4.1 Material obtained in the course of criminal investigations and which may be relevant to the investigation must be recorded and retained in accordance with the Criminal Procedure and Investigations Act 1996.

2.4.2 The councils must have in place arrangements for handling, storage and destruction of material obtained through the use of covert surveillance and compliance with the appropriate data protection requirements must be ensured.

2.4.3 Decisions on requests for judicial approval, authorisations, requests for authorisation, renewals, and cancellations are confidential material. The documents and any information contained therein must not be disclosed to any person who has no legitimate need to have access to the document, or to the information that it contains.

2.4.4 Authorising Officers must ensure that there are proper arrangements within their departments or services for the retention and security of such documents in accordance with the requirements of the current data protection legislation.

2.4.5 Such documents may need to be securely kept for a period (considered appropriate by the relevant head of service) following the completion of any surveillance, as they may have to be produced in court, or to the other party in court proceedings as part of legal disclosure requirements. Superfluous copies should not be made or kept.

3 Where we cannot use surveillance

3.1.1 There are some instances where surveillance is not permissible in any circumstances.

3.2 Intrusive Surveillance.

3.2.1 This is covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle, whether by way of a person or device. It will also be intrusive surveillance where a device placed outside consistently provides information of the same or equivalent quality and detail, as might be expected if it were in the premises or vehicle.

3.2.2 Residential premises are any part of premises occupied for residential purposes or living accommodation, including hotel rooms or prison cells. However, it does not include common areas in blocks of flats and similar premises.

3.2.3 Private vehicle is a vehicle used primarily for private purposes by the owner or person entitled to use it.

3.3 Use of Children to gather information about parent/ guardian

3.3.1 Authorisation may not be granted for the conduct or use of a source under the age of sixteen where it is intended that the purpose is to obtain information about their parent or any person who has parental responsibility for them.

3.4 Vulnerable Individuals

3.4.1 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 themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an individual may be vulnerable, they will only be authorised as a CHIS in the most exceptional of circumstances.

4 Communications data and recording telephone conversations

4.1.1 See details in section 10 of the RIPA policy which covers acquisition and disclosure of communications data. Local authorities are able to access certain types of communications data for the purpose of preventing or detecting serious crime or preventing or detecting crime or preventing disorder.

4.1.2 Applications no longer need Magistrate or Justice of the Peace approval, but must be processed through the National Anti- Fraud Network (NAFN), who will consider the application prior to submitting this for approval to the Office for Communications Data Authorisations ('OCDA').

4.2 Recording telephone conversations covertly

4.2.1 Council staff are not permitted to covertly record telephone conversations as such a covert activity is outside the powers of a Local Authority.

5 Use of Covert Human Intelligence Sources (CHIS)

5.1.1 The use of a covert human intelligence source (CHIS), and his or her conduct, would require authorisation under RIPA. In practice, it is unlikely that there will be any circumstances which would require the council to either use a CHIS or operate under cover in the manner of a CHIS, and advice should be sought from the RIPA Coordinating Officer or the Senior Responsible Officer before any authorisation is applied for or granted.

5.1.2 Further detail for the process is set out in the flowchart in section 19.

5.1.3 A CHIS is defined as the use or conduct of an individual who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information. These provisions would cover the use of professional witnesses to obtain evidence or information, or officers operating 'under cover'. Great caution should be exercised in these circumstances and the authorising officer must be satisfied that the authorisation is necessary, that the conduct authorised is proportionate to what is sought to be achieved and that arrangements for the overall management and control of the individual are in force.

5.1.4 The provisions of RIPA relating to CHIS do not apply where a situation would not normally require a relationship to be established for the covert purpose of obtaining information. For example: where members of the public volunteer information to the council as part of their normal civic duties; or where members of the public are asked to keep diaries of incidents in relation to, say, planning enforcement, anti-social behaviour or noise nuisance.

5.1.5 If a CHIS is used, both the use of the CHIS and his or her conduct require prior authorisation.

5.1.6 Where engaged, the Home Office Code of Practice on Covert Human Intelligence Sources (2018) requires public authorities to ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in the Act for each CHIS. This is known as a 'handler' and the officer will have day to day responsibility for dealing with the CHIS on behalf of the authority concerned; directing the day to day activities of the CHIS; recording the information supplied by the CHIS; and monitoring the security and welfare of the CHIS.

5.1.7 The handler of a CHIS will usually be of a rank or position below that of the Authorising Officer.

5.1.8 In addition to a handler, a 'controller' will also be appointed. This officer will be responsible for the management and supervision of the handler and general oversight of the use of the CHIS.

5.1.9 In view of the rigorous nature and importance of these requirements it is essential that CHIS activity is not undertaken by or on behalf of the council except under the strict control and supervision of officers who have been properly and recently trained for the specific purpose.

6 Directed Surveillance

6.1.1 As this activity is the most likely to be carried out, this procedure addresses this activity in more detail. Where there is to be directed surveillance written authorisation must be obtained in accordance with the provisions of RIPA before the surveillance commences.

6.1.2 Further detail for the process is set out in the flowchart in section 20.

6.1.3 Directed surveillance is defined as surveillance which is covert, but not intrusive and which is undertaken for the purposes of a specific investigation, and which is likely to result in obtaining private information about a person and which is carried out otherwise than as an immediate response to events where it would be impracticable to obtain prior authorisation. Therefore, investigating officers need to consider a number of key questions to determine whether a proposed activity falls within this definition of directed surveillance:

6.2 Is the proposed activity surveillance?

6.2.1 "Surveillance" includes:

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations or their other activities or communications
- recording anything monitored, observed or listened to in the course of surveillance
- Surveillance by, or with, the assistance of a surveillance device, which will include cameras, video, and listening or recording devices.

6.3 Is the surveillance covert?

6.3.1 Surveillance is covert where it is carried out in a manner calculated to ensure that the subjects of the surveillance are unaware that it is or may be taking place. It is therefore the intention of the officer carrying out the surveillance which is relevant to this issue of covertness.

6.4 Is the surveillance for the purposes of a specific investigation?

6.4.1 General observation, not forming part of any investigation into suspected breaches of the law and not directed against any specific person or persons is not directed surveillance e.g. CCTV cameras in council car parks are readily visible and if they are used to monitor the general activities of what is happening within the car park, it falls outside the definition.

6.4.2 If, however, the cameras are targeting a particular known individual, the usage will become a specific operation which will require authorisation.

6.5 Is the surveillance undertaken in such a manner that is likely to result in the obtaining of private information about a person?

6.5.1 "Private information" is any information concerning a person's private or family life. Whether information is personal in nature is relevant when deciding whether information is private.

6.5.2 The fact that observation of individuals occurs from the public highway will not prevent the discovery of private information.

6.5.3 When officers consider this question they should give due weight to the probability of discovering such information, as authorisation is not required if there is only a slight possibility of discovering private information.

6.6 Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to obtain prior authorisation?

6.6.1 If the surveillance is an immediate response to something happening during the course of an officer's work, it would not be reasonable to obtain prior authority. If this occurs, the officer must report the incident back to an authorising officer so a note can be made on the relevant department file and the central register.

6.7 Is the surveillance intrusive?

6.7.1 The council is not authorised to carry out intrusive surveillance, but in any event it is extremely unlikely that the council would contemplate undertaking this activity.

6.7.2 Surveillance is intrusive surveillance if it is carried out covertly in relation to anything taking place on residential premises or in a private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by a surveillance device.

7 Online covert activity / Use of internet and social media

7.1.1 Although social networking and internet sites are easily accessible, if they are going to be used during the course of an investigation, consideration must be given about whether a RIPA authorisation should be obtained.

7.1.2 Viewing of open-source material does not require authorisation unless and until it is repeated or systematic, at which stage directed surveillance authorisation should be considered.

7.1.3 Passing an access control so as to look deeper into the site, for example by making a 'friend request', requires at least directed surveillance authorisation. If the investigator is to go further and pursue enquiries within the site, thereby establishing a relationship with the site host in the guise of a member of the public, this requires CHIS authorisation.

7.1.4 Further guidance with illustrative examples is provided in the Home Office's *Revised Code of Practice on Covert Surveillance and Property Interference* in the section on *Online Covert Activity*, pages 18-21 at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

7.1.5 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where the council may have taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available (required).

7.1.6 Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

7.1.7 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

7.1.8 Whether there may be interference with a person's private life includes a consideration of the nature of the councils' activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where there is systematic collection and recording of information about a particular person or group, a directed surveillance authorisation should be considered.

7.1.9 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or group;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include personal information and therefore constitute collateral intrusion into the privacy of these third parties.

8 Rules of evidence

8.1.1 Material obtained through covert surveillance may be used as evidence in criminal proceedings. Provided that surveillance has been properly authorised, the evidence gathered should be admissible under law and in accordance with Section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

8.1.2 Material gathered as a result of surveillance authorised under the Act is subject to the ordinary rules for retention and disclosure of material and the Criminal Procedure and Investigations Act 1996.

9 Authorisations

9.1.1 Authorisation must be given in writing.

9.1.2 Authorising officers should not ordinarily give authorisations in investigations or operations in which they are directly involved unless this is unavoidable.

9.1.3 No Authorising Officer shall grant an authorisation for the carrying out of directed surveillance or the use of a CHIS unless they believe:

a) that an authorisation is necessary for the purpose of preventing or detecting crime, and in the case of directed surveillance that the offence in question carries a maximum sentence of at least six months imprisonment or relates to the sale of alcohol or tobacco to persons who are underage; and

b) the authorised activity is proportionate to what is sought to be achieved by carrying it out.

9.1.4 The contemplated activity must be considered necessary in the particular circumstances of the case. Authorisation can only be granted where there is justifiable interference with an individual's human rights, i.e. it is necessary and proportionate for surveillance activities to take place

9.1.5 Proportionality is a key concept of RIPA. An authorisation should demonstrate how an authorising officer has reached the conclusion that the surveillance activity is proportionate to what it seeks to achieve, including an explanation of the reasons why the method, tactic or technique is not disproportionate (the proverbial 'sledgehammer to crack a nut').

9.1.6 Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, tactic or technique is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of authorisation have been fully considered.

9.1.7 An aide memoire for factors to consider in proportionality and intrusiveness is included in section 22.

9.1.8 Before authorising surveillance, the authorising officer must also take into account the risk of intrusion into the privacy of persons other than those who are the target of the investigation. This is known as collateral intrusion. The authorisation procedures allow for an assessment of collateral intrusion which the authorising officer will be required to consider prior to granting authorisation. In order to decide whether to grant authorisation the authorising officer must have a full picture of the operation, the proposed method(s) of observation and the Human Rights Act implications of the operation.

9.1.9 A potential model authorisation would make clear that the following elements of proportionality had been fully considered:

a) balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
b) explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,
c) that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
d) providing evidence of other methods and why they were not implemented.

9.1.10 At the point in time immediately before the completion of the application for a RIPA authorisation and before it is presented to the Authorising Officer for his/her authorisation, the application should be delivered to the RIPA Coordinating Officer. This is to assist with the completion of the central record of authorisations and to provide for an additional element of 'quality control' over the content of the application. Assuming it is granted by the Authorising Officer, the completed authorisation should also be returned to the RIPA Coordinating Officer and again assessed for quality before arrangements are made for a Magistrates Court to consider its approval (see the judicial approval section below).

10 Judicial approval of RIPA authorisations

10.1.1 In addition to the pre-conditions and requirements for authorisations described above, no authorisation for directed surveillance or the use of a CHIS will take effect unless and until the relevant judicial authority (i.e., a Magistrate) has made an order approving the grant of the authorisation. It is therefore vital that any surveillance for which authorisation has been sought does not start until such time as it has been approved by a Magistrate.

10.1.2 It is necessary for the council to obtain judicial approval for all initial RIPA authorisations/applications and renewals. There is no requirement for a Magistrate to consider either cancellations or internal reviews.

10.1.3 The need for judicial approval from a Magistrate will require the RIPA Coordinating Officer or another lawyer under their supervision to contact the administration section at the local Magistrates Court to request a hearing for this stage of the authorisation. In advance of the hearing, the Authorising Officer should provide to the court the RIPA authorisation signed by him/her and a completed judicial application/order form, together with any other relevant supporting documents. The hearing to consider the application will be held in private, and the Magistrate will consider the documentation provided, and ask questions to clarify points or gain reassurance on any matters of interest or concern. Ordinarily, the person representing the council at this hearing will be the Authorising Officer, and this person should make sure that s/he takes to the hearing evidence of his/her own authorisation to grant authorisations and represent the council in court proceedings.

10.1.4 The judicial approval process is set out in the workflow in section 21, guidance and approval/order forms can be found on the Gov.uk website.

11 Senior Responsible Officer's role

11.1.1 The Council's Senior Responsible Officer (SRO) is the Head of Legal and Democratic. The SRO is responsible for:

- The integrity of the process in place within the councils for the management of Covert Human Intelligence Sources and Directed Surveillance
- Compliance with Part II of RIPA and the Codes of Practice
- Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections
- Oversight of the implementation of any post-inspection action plan approved by the IPCO
- Ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports by the Investigatory Powers Commissioner's Office.
- Presenting the policy on an annual basis to the Joint Audit and Governance Committee for review

11.2 Specific responsibilities

11.2.1 Submitting annual statistics to the IPCO in relation to authorisations.

11.2.2 Communicating to the IPCO any unauthorised activity that might come to the attention of the authority. This must be done within 5 working days. The records, documentation, and associated documentation relating to this unauthorised activity must be retained by the Senior Responsible Officer and disclosed to the IPCO upon request, and certainly to an inspector from the IPCO at the commencement of the next scheduled inspection.

11.2.3 Ensuring a central register of authorisations and approvals is maintained. This is actioned through the RIPA Co-ordinator,

12 Authorising officers

12.1.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No 521 prescribes the Authorising Officer must be at least a director, head of service, service manager or equivalent.

12.1.2 Under the constitution's scheme of delegation, heads of service and the Chief Executive have delegated authority to issue RIPA authorisations, however further important provisions about Authorising Officers and about training are contained in section 7 below. For a service manager to become an Authorising Officer, a written authority must be produced by the relevant head of service.

12.1.3 The Authorising Officer should not be part of the surveillance team. S/he cannot grant a self-authorisation, and in the event that a head of service wishes to undertake the surveillance personally, or as part of the surveillance team, any authority should be issued by a different Authorising Officer.

12.1.4 Authorising Officers must be aware of the requirements of RIPA and how to properly consider requests for authority. Authorising Officers must demonstrate that these requests have been properly considered when they complete the authorisation form.

12.1.5 Where the surveillance is likely to lead to the obtaining of "confidential information" (as defined below), a RIPA authorisation can only be given by the Chief Executive (or in his absence, his deputy). For these purposes confidential information has the following specific meaning, namely:

a) legally privileged information e.g. communications between a professional legal adviser and a client

b) confidential personal information, which is information kept in confidence and relating to a person's physical or mental health or relating to spiritual counselling given to a person e.g. consultations between a health professional and a patient, information from a patient's medical records or conversations between an individual and a Minister of Religion

c) confidential journalistic information, held for the purposes of journalism on the basis that it or its source would not be revealed.

12.1.6 It is difficult to envisage circumstances in which the council's investigative activities would either require, justify or otherwise result in the obtaining of confidential information and if any such information is obtained during surveillance, legal advice should be sought immediately.

13 Training

13.1.1 The council will ensure that adequate training takes place for Authorising Officers and investigating officers. Such training may be arranged and provided through officers' own professional associations or through the use of outside agencies.

13.1.2 Sharing training with other local authorities may also be appropriate. The council's legal services team can also assist with training and by giving guidance from time to time, either generally as legislation/guidance evolves or in specific cases.

13.1.3 As it is especially important for Authorising Officers to be able to demonstrate an up to date knowledge of RIPA and best practice, the delegation to grant authorisations should generally be exercised only by those officers who have undertaken and kept up to date RIPA training.

13.1.4 In order to assist this process, the Council's RIPA Coordinating Officer under the general supervision of the Senior Responsible Officer for RIPA will maintain, monitor and review a central record of RIPA training attended by officers of the council along with a list of those officers who have undertaken training necessary to enable them to assess and grant authorisations.

13.1.5 It should further be noted that advice from the Investigatory Powers Commissioner's Office (IPCO) is that officers engaged in RIPA activity and/or management should receive training appropriate to their roles at approximately 18 month intervals.

14 Authorisation forms

14.1.1 RIPA itself does not contain prescribed forms of authorisation. However, the adapted Home Office model forms referred to below should be used. This will ensure a consistent approach is adopted across service teams and ensure all relevant issues are addressed during the decision-making process.

14.1.2 Links to the forms below can be found at https://www.gov.uk/government/collections/ripa-forms--2

14.2 Forms for directed surveillance:

- Application for use of directed surveillance
- Renewal form for directed surveillance
- Review of use of directed surveillance
- Cancellation of use of directed surveillance

14.3 Forms for CHIS:

- Application for the use of CHIS
- Reviewing the use of CHIS
- Renewal of authorisation to use CHIS
- Cancellation of CHIS

15 Duration of authorisation, reviews and renewals

15.1 Duration of authorisation

15.1.1 A written authorisation for directed surveillance ceases to have effect unless renewed and approved at the end of a period of three months beginning from the date on which it took effect (12 months in the case of a CHIS authorisation).

15.1.2 Officers should ensure authorisations only last for as long as is considered necessary and proportionate.

15.2 Reviews

15.2.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. It is the responsibility of the Authorising Officer to determine how often a review should take place and this should be as frequently as is considered necessary and practicable. The frequency of reviews must be specified on the authorisation form.

15.2.2 The results of a review should be recorded in the central record of authorisations. Particular attention should be paid to reviews where the surveillance provides access to confidential information or involves collateral intrusion.

15.3 Renewals

15.3.1 If at any time before an authorisation would cease to have effect the Authorising Officer considers it necessary for the authorisation to continue for the purpose of which it was given, they may renew it in writing for a further period of three months.

15.3.2 Magistrate approval, if necessary, must then be obtained prior to expiry of the original authorisation in order for activity to continue.

15.3.3 Any time before the authorisation would cease to have effect, the Authorising Officer may renew, in writing, it is still considered necessary.

15.3.4 Authorisations may be renewed more than once provided they continue to meet the criteria for authorisations. The renewal does not have to be authorised by the same authorising officer who granted the original authorisation.

15.3.5 The Authorising Officer who granted the authorisation or last renewed the authorisation must cancel it if satisfied the directed surveillance no longer meets the criteria upon which it was authorised.

15.3.6 Renewal records should be kept as part of the central record of authorisations.

16 Cancellations and ceasing surveillance activity

16.1 Cancellations

16.1.1 The authorising officer who granted or last renewed the authorisation must cancel it as soon as it no longer meets the criteria for which it was originally authorised. In any event, it will expire after 3 months (12 months for CHIS).

16.1.2 Where the authorising officer is no longer available the person who is taking over that role will be responsible.

16.2 Ceasing surveillance activity

16.2.1 As soon as the decision to cease directed surveillance is taken, all those involved must be directed to stop surveillance of the subject.

16.2.2 The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation where relevant.

17 Codes of practice

17.1.1 The Home Office has published a Code of Practice on Covert Surveillance and Property Interference (December 2022) and a Code of Practice on Covert Human Intelligence Sources (December 2022) which provide further guidance on the use of these activities.

17.1.2 These codes are available on the Gov.uk website and should be read by investigating officers and team leaders whose investigations may involve covert surveillance.

17.1.3 The codes of practice are admissible as evidence in criminal and civil proceedings. The councils will normally follow the requirements of codes of practice issued by the Home Secretary unless there are exceptional circumstances justifying a departure from the recommended approach.

17.1.4 The IPCO also produces guidance from time to time on procedures and oversight arrangements for local councils on RIPA and its website offers a further valuable reference source.

18 Officers with designated RIPA roles

18.1 Senior Responsible Officer

18.1.1 Head of Legal and Democratic

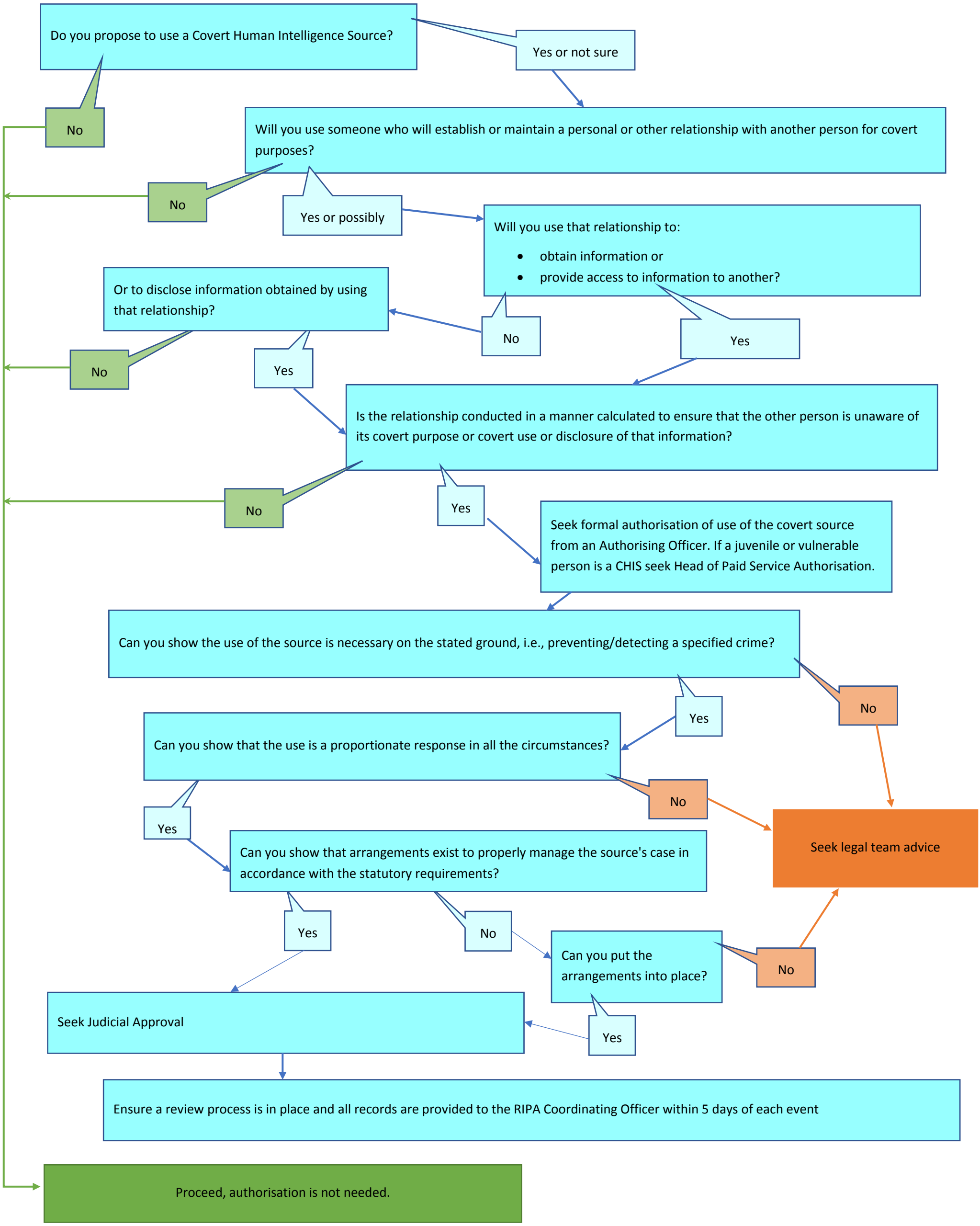
18.2 RIPA Co-ordinating Officer

18.2.1 Deputy Head of Legal (Operational)

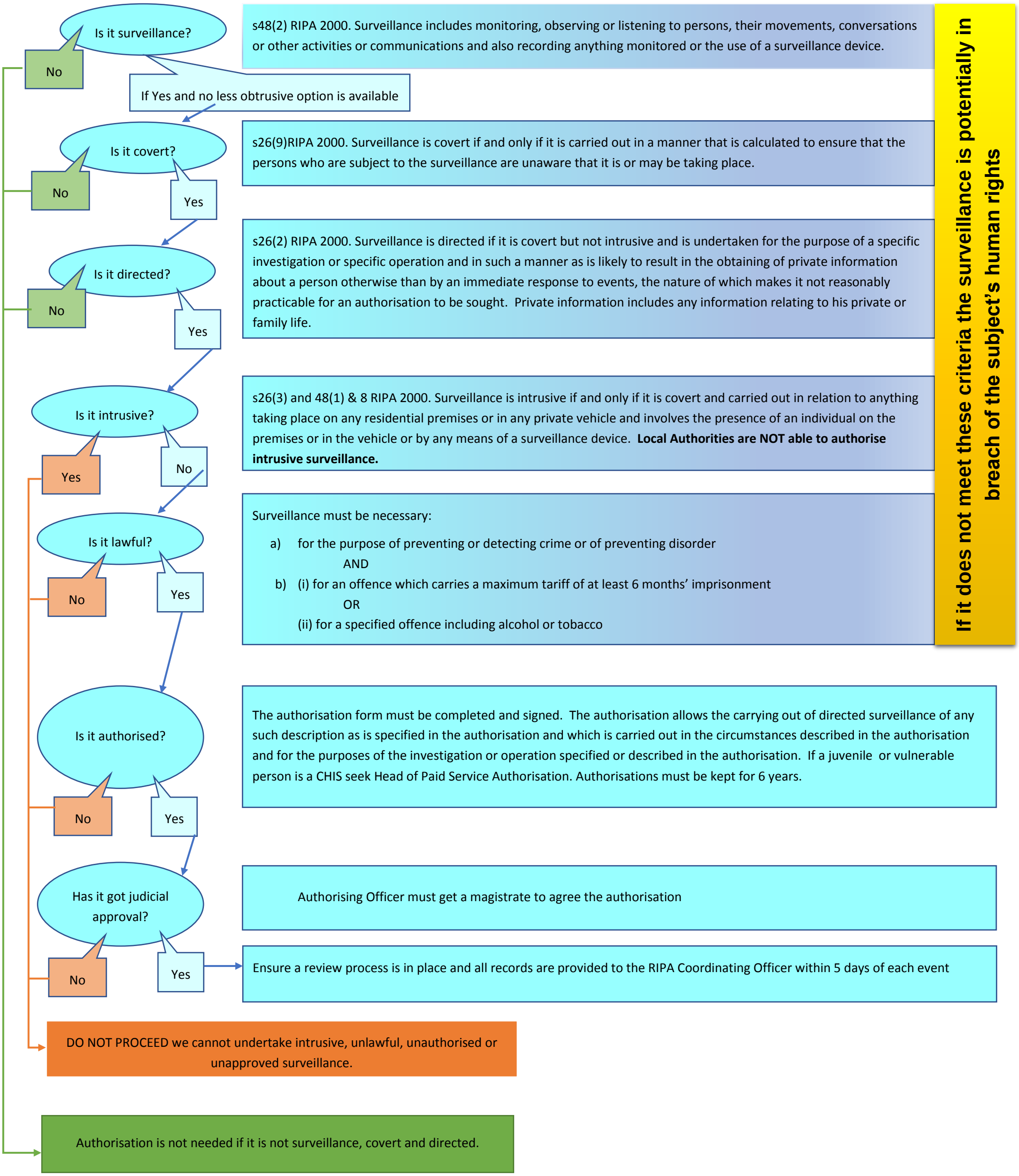
18.3 Authorising officers

18.3.1 Deputy Chief Executive - Partnerships

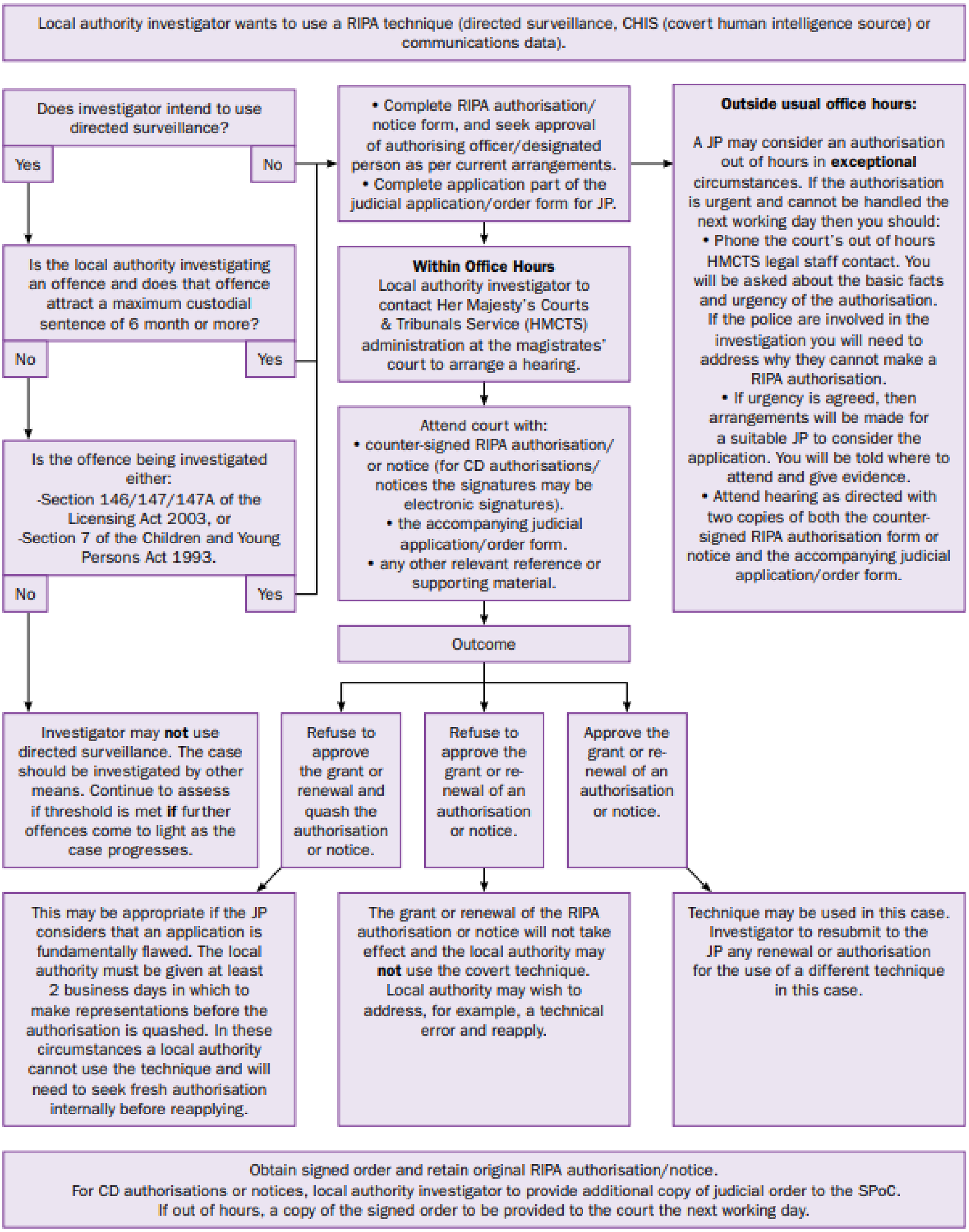
19 **FLOWCHART** - Covert Human Intelligence Sources (CHIS) Process



20 **FLOWCHART** - Directed Surveillance Process



21 **FLOWCHART -** Application to a Justice of the Peace Seeking an Order to Approve the Grant of a RIPA Authorisation or Notice



22 AIDE MEMOIRE – Factors to consider in proportionality and intrusiveness

22.1.1 The following assumes the cases for necessity and resources have already been made. **Factors in bold and starred (*) usually carry more weight.**

22.2 Factors relevant to data collection and analytics

Value	
Timeliness and need *	• **gravity and extent of (potential) crime or harm** • **public interest** • **urgency of need**
Function *	• **for analysis of the data on its own** • **to enrich existing data** • **to become enriched by existing data** • **for training sets for use in machine learning algorithms in established tools** • **for use in development or enhancement of a new capability or tool, which may be a prototype**
Relevance and marginal benefits *	• **to given investigation(s)** • **to other data available**
Impact of time and place	• dependencies such as when and where data were collected
Type of data or collection method	• new or existing type of data • new, more accurate, or existing collection method
Volume	
Amount *	• **fixed and known before collection** • **unknown but can be approximated** • **granularity and uncertainties of approximations including dependencies**
Frequency	• one-time collection • repeated collection, how many times and at which intervals • continuous collection, for how long • how does the amount of data held vary over time
Data Management	
Storage	• where, how, and under whose authority • length of time planned retention, for which parts • security of access and resilience to loss or corruption
Deletion and manipulation	• plans and mechanisms for indexing, deletion and/or putting beyond use, redaction, and abstraction
Analysis	
Human and/or machine inspection (*)	• **uncertainty (false positives/negatives) thresholds for human and machine inspection** • **risks of bias for human and machine inspection** • **human only inspection is possible of entire data set** • **machine only inspection is possible of entire data set** • **primary analysis by machine inspection to extract set for secondary analysis by human inspection**
Alternatives	
What other methods have been considered	• if they have been implemented successfully, why are they not employed now • if they have not been implemented successfully, why not • opportunity cost - what will be lost by implementing this method over others • efficiency and effectiveness of proposed method vs. alternatives

22.3 Factors relevant to intrusiveness

Privacy Intrusion	
Type (*)	• **degrees of foreseeable, targeted, collateral, and privileged intrusion – how many individuals** • **their interrelationships and dependencies**
Sensitivity (*)	• **degree of sensitivity of the data collected and/or what will be revealed through subsequent analytics**
Scaling	• how the intrusion scales from individuals to different populations e.g. multiplicative, additive, constant • how the intrusion affects a community defined by a characteristic
Access	• breadth of people (e.g. analysts) and systems that will have access either directly to the data collected or indirectly via analytical tools • breadth of people (e.g. analysts, colleagues, managers) who will have access to reports that refer to the data

Regulation of Investigatory Powers Act (RIPA) action plan – March 2024

Objective 1. Policy, procedures and documents:

Action	Action owner	Target date	Comments	Completed date
1.1 Add the escalation in the authorisation level for Juvenile and Vulnerable CHIS and the variation of the authorisation period for a Juvenile CHIS (May 2021 action)	RIPA Senior Responsible Officer (Head of Legal and Democratic)	Revised to April 2024	Added into revised policy and procedures which is to be presented to Joint Audit and Governance Committee 15th April 2024	
1.2 Add fuller explanation of IPCO's full oversight role (May 2021 action)	RIPA Senior Responsible Officer (Head of Legal and Democratic)	Revised to April 2024	Added into revised policy and procedures which is to be presented to Joint Audit and Governance Committee April 2024	
1.3 Add explanation of FOI Act and requests for disclosure of IPCO inspection reports needing IPCO DPO consultation, as per IPCO Spring 2023 newsletter		Present to April 2024 JAGC for policy review.	Added into revised policy and procedures which is to be presented to Joint Audit and Governance Committee April 2024	
1.4 Ensure policy covers data handling, retention, review and destruction (see IPCO annual report page 94)		Present to April 2024 JAGC for policy review.		

includes compliance assurance to JAGC annually				

Objective 2. Training and awareness:

Action	Action owner	Target date	Comments	Completed date
2.1 Deliver RIPA update training for investigating and legal officers (May 2021 action)	RIPA Co-ordinator (Deputy Head of Legal (Operational)	May 2021	Training delivered by Ben Fullbrook of Landmark Chambers. Invitations extended to approximately 30 investigating and legal officers who either attended the online session or (along with other officers) have the opportunity to watch the recording. Further training for officers being arranged with Cornerstone Chambers for April 2024	13 May 2021
2.2 Deliver training specifically for RIPA authorising officers	RIPA Co-ordinator (Deputy Head of Legal (Operational)	December 2021 Revised to April 2024	Dependent upon the review and confirmation of new authorising officers by the Strategic Management Team	
2.3 Deliver refresher training for investigating and legal officers and authorising officers	RIPA Co-ordinator (Deputy Head of Legal (Operational)	January 2025 and annually		

2.4 Develop a plan for raising RIPA awareness across the organisation to improve compliance and prevent unauthorised activity, including consideration of targeted briefings of relevant teams and general staff updates	RIPA Co-ordinator (Deputy Head of Legal (Operational))	April 2024 and annually	Signposting policy and procedures to all via Intranet and staff news letter April 2024	
2.5 Ensure service areas are clear in what actions are acceptable before RIPA should be considered for use of internet as part of investigations. (see page 93 of IPCO annual report from march 2023)	RIPA Co-ordinator (Deputy Head of Legal (Operational)	April 2024 and annually		

Objective 3. Records management:

Action	Action owner	Target date	Comments	Completed date
3.1 Add the product of directed surveillance to the corporate/services guidance on data	RIPA Senior Responsible Officer	April 2024		

management, records of processing activities and retention policies and update the RIPA policy and procedures as required.	(Head of Legal and Democratic)			
3.2 Consider incorporating the management of such product within the Central RIPA Register	RIPA Senior Responsible Officer (Head of Legal and Democratic)	March 2024	Discussed and agreed draft changes now being prepared	