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

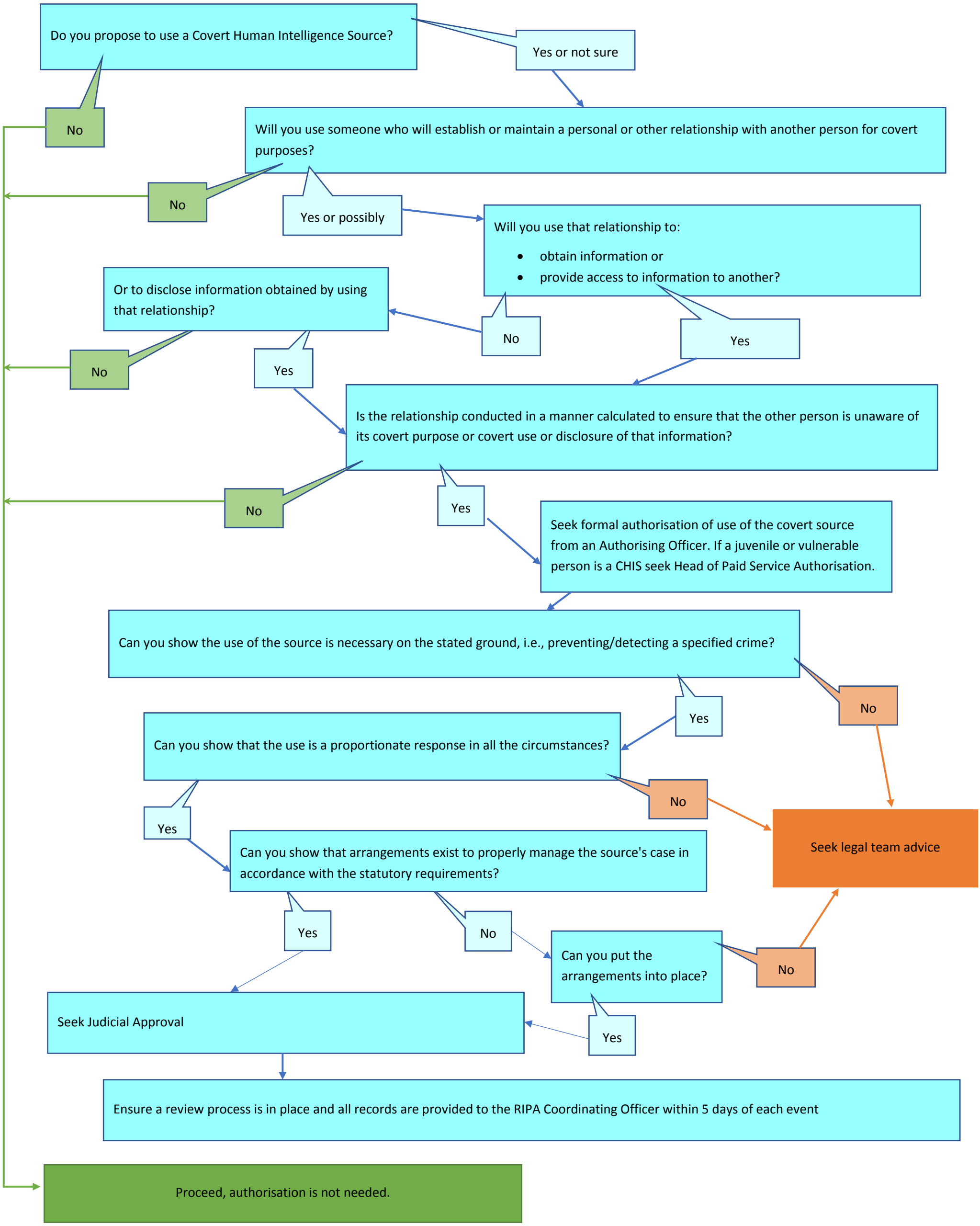
18.2 RIPA Co-ordinating Officer

18.2.1 Deputy Head of Legal (Operational)

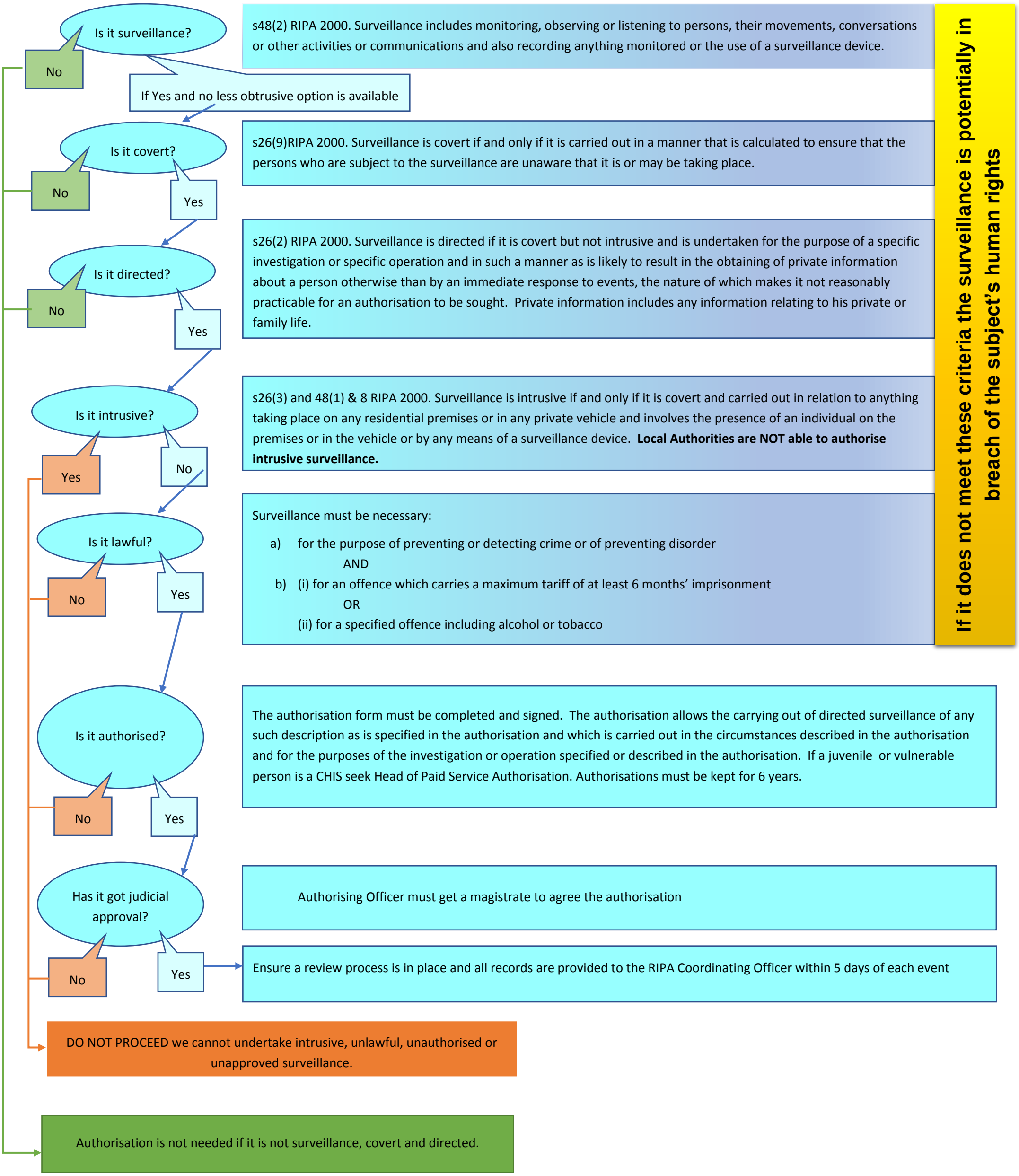
18.3 Authorising officers

18.3.1 Deputy Chief Executive - Partnerships

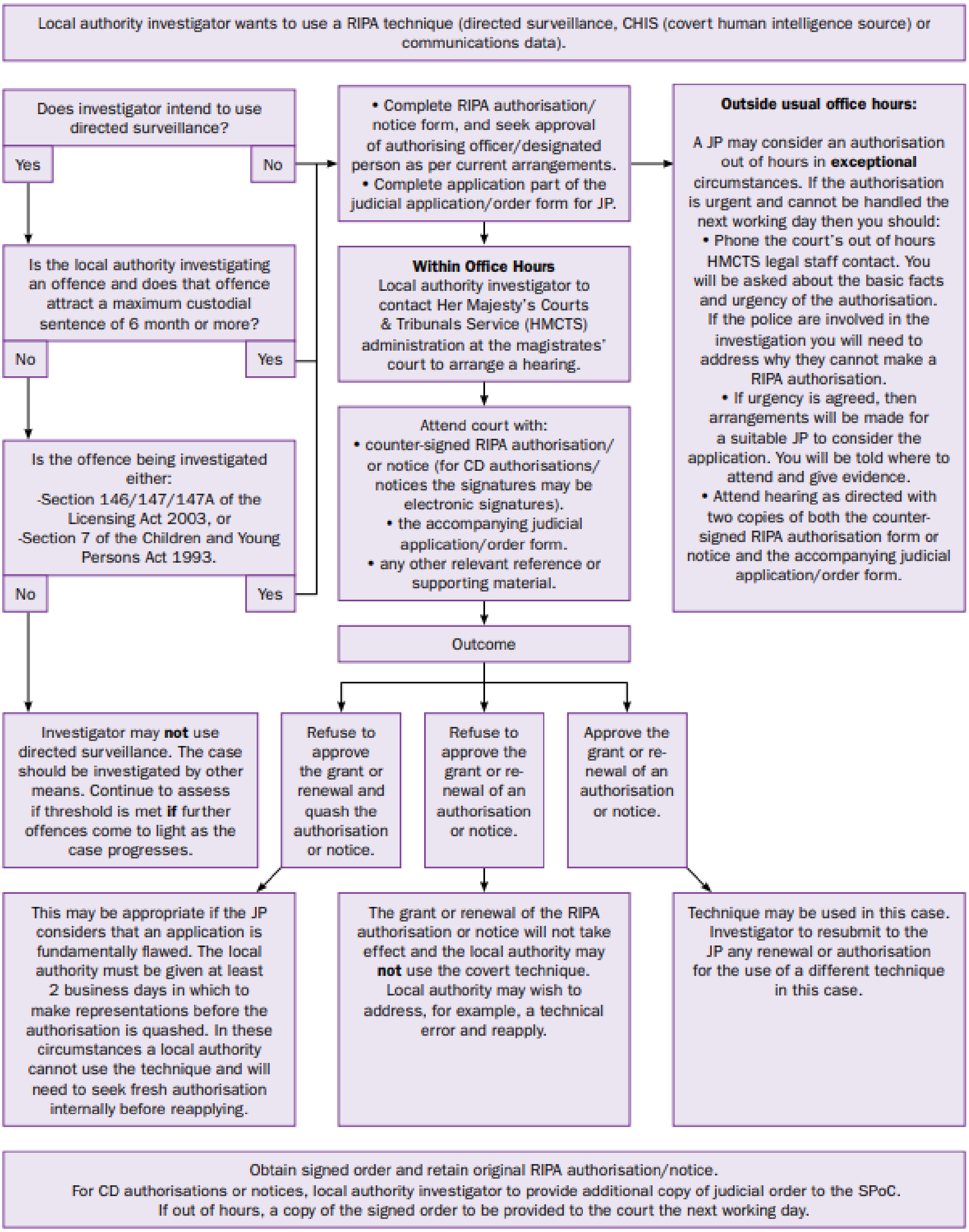
19 **FLOWCHART** - Covert Human Intelligence Sources (CHIS) Process



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