

# **CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATOR POWERS ACT 2016**

<b>Version No.</b>	<b>Author</b>	<b>Date</b>
See Page 19		
1.1	Kerryn Woolett	May 2020
1.2	Kerryn Woolett	June 2021

**Version 1.2  
June 2021**

	<b>Contents</b>	<b>Page No.</b>
1.	Introduction	3
2.	Types of Surveillance	4
3.	Conduct and Use of Covert Human Intelligence Sources	5
4.	Open Source (Online) Covert Activity	6
5.	Use of Personal Devices for Business Use	7
6.	The Council Owned Drone	7
7.	Local Authority Directed Surveillance Crime Threshold	7
8.	Authorisation Process - Directed Surveillance and Use of a CHIS	7
9.	Communications Data	11
10.	Authorisation Process - Communications Data	12
11.	Central Co-ordination	16
12.	Working with Other Agencies	17
13.	Other Sources of Information	17
14.	Records Management	17
15.	Revision History	19

## CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATORY POWERS ACT 2016

### 1. INTRODUCTION

- 1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) is concerned with the regulation of surveillance and other intelligence gathering by public authorities in the conduct of their legitimate business.
- 1.2 The Investigatory Powers Act 2016 (IPA) sets out the extent to which certain investigatory powers may be used to interfere with privacy. In particular about the interception of communications, equipment interference and the acquisition and retention of **communications data**.
- 1.3 Section 6 of the Human Rights Act 1998 provides that it is unlawful for a public authority to act in a way which is incompatible with a European Convention right. Article 8 of the European Convention on Human Rights says that everyone has the right to respect for their private and family life, their home and their correspondence.
- 1.4 The use of surveillance and other intelligence gathering techniques may amount to an interference with rights protected by Article 8 of the European Convention on Human Rights and could amount to a violation of those rights unless the interference is in accordance with the law.
- 1.5 The aim of RIPA and the IPA is to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action. RIPA provides a statutory framework for the authorisation of certain types of **covert** intelligence gathering which is consistent with the Human Rights Act 1998 and the European Convention on Human Rights. Similarly, the IPA provides a statutory framework for the lawful interception and use of **communications data**.
- 1.6 The Council has approved a policy for tackling fraud and corruption. In limited circumstances the Council may wish to use surveillance techniques or **communications data** for the purpose of enforcing this policy or other of its statutory functions. The requirements of RIPA and the IPA are most likely to apply to those sections of the Council with enforcement / investigatory functions.
- 1.7 Section 27 of RIPA provides that conduct authorised under RIPA will be "lawful for all purposes." This means a person authorised under RIPA is entitled to engage in the conduct which has been authorised under RIPA and the Council will be protected from challenges to both the gathering of, and the subsequent use of, covertly obtained information enabling the Council to show that it has acted lawfully.
- 1.8 RIPA also provides a statutory mechanism for authorising the use of a "**covert human intelligence source**", e.g. undercover agents.
- 1.9 The IPA permits access to **communications data** in specific circumstances.
- 1.10 Non-compliance with RIPA or the IPA may result in:
  - 1.10.1 evidence being disallowed by the courts;
  - 1.10.2 a complaint to the Investigatory Powers Commissioner's Office;

- 1.10.3 a complaint to the Local Government and Social Care Ombudsman; and/or
- 1.10.4 the Council being ordered to pay compensation.

It is essential therefore that the Council's policies and procedures, as set out in this document, are followed. A flowchart of the procedures to be followed is at Appendix 1.

## 2. TYPES OF SURVEILLANCE

- 2.1 Surveillance includes monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It also includes recording any of the aforementioned activities.
- 2.2 Surveillance may be "**overt**" or "**covert**".
- 2.3 Surveillance will be "**overt**" if the act of surveillance is not calculated to be hidden from view, even if the motives of the person undertaking the surveillance remain concealed.
- 2.4 Most of the surveillance carried out by the Council is done overtly – there is nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public, and/or will be going about Council business openly. Similarly, surveillance will be **overt** if the subject has been told it will happen (e.g. where a noisy householder is warned that noise will be recorded if it continues).
- 2.5 Surveillance is "**covert**" if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. RIPA regulates two types of **covert** surveillance.
- 2.6 The first type of **covert** surveillance is "**directed surveillance**". "**Directed surveillance**" means surveillance that is:
  - 2.6.1 **covert**;
  - 2.6.2 not intrusive;
  - 2.6.3 undertaken for the purposes of a specific investigation or specific operation;
  - 2.6.4 undertaken 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
  - 2.6.5 undertaken 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 RIPA to be sought for the carrying out of the surveillance.
- 2.7 RIPA states that "**private information**" includes any information relating to a person's private or family life. The Home Office Covert Surveillance and Property Interference Revised Code of Practice (latest edition at time of writing was August 2018) states that as a result, "**private information**" is capable of including any aspect of a person's private or personal relationship with others, such as family (which should be treated as extending beyond the formal relationships created by marriage or civil partnership) and professional or business relationships.

- 2.8 RIPA sets out a number of grounds on which an authorisation for **directed surveillance** can be considered necessary. In the case of a Local Authority, only one of these grounds is applicable, that ground is that **directed surveillance** is necessary “for the purpose of preventing or detecting crime or of preventing disorder”.
- 2.9 The fact that **covert** surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will usually result in the obtaining of private information about that person as well as others that he or she comes into contact or associates with.
- 2.10 An example of **directed surveillance** would be when officers follow a person over a period of time to find out whether they are working at the same time as claiming benefit. Similarly, although town centre CCTV cameras will not normally require a RIPA authorisation, if a camera is directed in such a way as to observe a particular individual, this would amount to **directed surveillance** and an authorisation would be required.
- 2.11 The second type of **covert** surveillance is “**intrusive surveillance**”. Surveillance is intrusive if, and only if, it 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.
- 2.12 A Local Authority cannot carry out **intrusive surveillance** under RIPA. **Intrusive surveillance** can only be carried out by the police and other law enforcement agencies.

### 3. CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

- 3.1 A person is a **Covert Human Intelligence Source (CHIS)** if he or she establishes or maintains a personal or other relationship with another person in order to covertly obtain or disclose information.
- 3.2 RIPA sets out special rules relating to the management and use of information supplied by a **CHIS** and a duty of care is owed to the **CHIS** in how the information is used.
- 3.3 The conduct or use of a **CHIS** requires prior authorisation. Again, the ground on which a **CHIS** may be used by a Local Authority is “for the purpose of preventing or detecting crime or of preventing disorder.”
- 3.4 A RIPA authorisation may not be required in circumstances where members of the public volunteer information to the Council as part of their normal civic responsibilities, however, this will depend on how the information has been obtained. If the person has obtained the information as an ‘insider’ i.e. in the course of a personal or other relationship or “as a result of the existence of such a relationship” then the person is likely to be a **CHIS**, even if the relationship was not formed or maintained for that purpose.
- 3.5 If the person has obtained the information as an outside observer then he or she is not a **CHIS**.
- 3.6 Where contact numbers are set up by the Council to receive information then it is unlikely that persons reporting information will be **CHISs** and similarly, people who complain about anti- social behaviour, and are asked to keep a diary, will not normally

be **CHISs** because they are not being required to establish or maintain a relationship for a **covert** purpose.

#### Juvenile CHISs

- 3.7 Special safeguards apply to the use or conduct of juveniles, that is, those under 18 years old, as a **CHIS**. On no occasion should the use or conduct of a **CHIS** under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.
- 3.8 Authorisations for juvenile sources should be granted by those listed in the table at Annex A of the Home Office Covert Human Intelligence Sources Revised Code of Practice (latest edition at time of writing was August 2018). In this Council, only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

#### **4. OPEN SOURCE (ONLINE) COVERT ACTIVITY**

- 4.1 The use of the internet may be required to gather information during an operation, which may amount to **directed surveillance**. The Home Office Covert Surveillance and Property Interference Revised Code of Practice (latest edition at time of writing was August 2018) advises that simple reconnaissance of websites, that is, preliminary examination with a view to establishing whether a 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. However, where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, a RIPA authorisation should be considered. When conducting an investigation which involves the use of the internet factors to consider are:
- officers must not create a false identity in order to "befriend" individuals on social networks without an authorisation under RIPA;
  - officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation;
  - repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once a RIPA authorisation has been granted and approved by a Magistrate; and
  - officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.
- 4.2 Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites without disclosing his or her identity, a **CHIS** authorisation should be considered.

## 5. USE OF PERSONAL DEVICES FOR BUSINESS USE

- 5.1 Use of a personal device to access the internet or social media for business use, for example, as part of investigation, is still captured by RIPA. Consequently, officers are advised not to use personal devices for business use, particularly using a personal device to access the internet and social media for business use.

## 6. THE COUNCIL OWNED DRONE

- 6.1 Use of a drone has the potential to capture **private information**. **Collateral intrusion** is also highly likely when using a drone. Therefore, consideration should be given to whether a RIPA authorisation is required. A drone can be a very useful tool to use in an investigation, however, if there is the potential to gather **personal information** the subject of the investigation and/or the landowner will either need to be notified of the use of the drone (such that any use of the drone is not covert) or a RIPA authorisation will be needed. If the drone is to be flown over a residential area or highly populated area, where the potential for **collateral intrusion** is high, notification that the drone will be used will be published on the Council's website prior to the flight.

## 7. LOCAL AUTHORITY DIRECTED SURVEILLANCE CRIME THRESHOLD

- 7.1 A **Crime Threshold** applies to the authorisation of **directed surveillance** by Local Authorities under RIPA (see article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010). This **Crime Threshold** does not apply to the authorisation of a **CHIS** by a Local Authority.
- 7.2 Local Authorities can only authorise use of **directed surveillance** under RIPA for the purpose of preventing or detecting criminal offences or disorder associated with criminal offences that are:
- 7.2.1 punishable, whether on summary conviction or on indictment, by a maximum term of at least six months imprisonment; or
- 7.2.2 relate to the underage sale of alcohol or tobacco.
- 7.3 If the **Crime Threshold** is not met, though surveillance is still required, a Non-RIPA form should be completed. A Non-RIPA form requires the applicant officer to consider necessity and proportionality as per a RIPA authorisation, however, there is no requirement for approval by a Justice of the Peace.

## 8. AUTHORISATION PROCESS - DIRECTED SURVEILLANCE AND USE OF A CHIS

### Stage 1 - Request for Authorisation

- 8.1 **Directed surveillance** or the use of a **CHIS** can only be authorised by a Local Authority if the authorisation is *necessary* for the purpose of preventing or detecting crime or preventing disorder and the authorised surveillance is *proportionate* to what is sought to be achieved by carrying the surveillance out. When authorising the use of a **CHIS** arrangements also need to be in place for management of the **CHIS** and to ensure the security and welfare of the **CHIS**.
- 8.2 For **directed surveillance** or the use of a **CHIS**, only the approved RIPA forms, available on the Home Office website

(<https://www.gov.uk/government/collections/ripa-forms--2>)

may be used. Any other form will be rejected by the Authorising Officer. The applicant officer should complete the appropriate form providing as much detail as possible then submit to the appropriate Authorising Officer for authorisation.

- 8.3 If in doubt about the process to be followed or the information required in the form, an applicant officer should always seek the advice of the Head of Legal and Commercial Services or the Audit Manager before applying for an authorisation under RIPA.
- 8.4 The applicant officer will be responsible for ensuring that copies of all forms are forwarded to the Audit Manager within seven days of issue. As a control measure the Audit Manager will supply the applicant officer with a referenced copy of the authorisation which they should keep in their department in secure storage. Officers should ensure that material passing between them is sent in such a way that it cannot be read or intercepted by other people.

### Stage 2 - Considering an Application for Authorisation

- 8.5 **Directed surveillance** or use of a **CHIS** can only be lawfully carried out if properly authorised and carried out in strict accordance with the terms of the authorisation.
- 8.6 The Secretary of State has specified by statutory instrument (the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010) that, for any district council in England, Directors, Heads of Service or Service Managers or equivalent are designated persons for the purpose of s.28 and s.29 of RIPA, that is, they may act as Authorising Officers for the purpose of authorising applications for **directed surveillance** or the use of a **CHIS**. In this Council, the Chief Executive and the Directors are designated to act as Authorising Officers under the Constitution (Part 3, Sec 7, Para 3.3). The Chief Executive or Monitoring Officer may designate other officers to act as Authorising Officers, provided these officers are of the level specified by the Secretary of State in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010.
- 8.7 Before signing a form seeking authorisation, the Authorising Officer must have regard to this Policy and Procedure, to any relevant Code of Practice, to any advice from the Head of Legal and Commercial Services or the Audit Manager and to any other relevant guidance.
- 8.8 The Authorising Officer must also satisfy himself / herself that the surveillance proposed in the application is:
  - 8.8.1 *in accordance with the law;*
  - 8.8.2 *necessary* in the circumstances of the particular case on the ground of preventing or detecting crime or preventing disorder; and
  - 8.8.3 *proportionate* to what it seeks to achieve.
- 8.9 In considering whether or not the proposed surveillance is proportionate, the Authorising Officer will need to consider:
  - 8.9.1 The seriousness of the crime or disorder which the surveillance seeks to detect and weigh this against the type and extent of surveillance proposed. For minor offences, it may be that surveillance is never proportionate; and



- 8.9.2 whether there are other more non- intrusive ways of achieving the desired outcome. If there are none, the Authorising Officer will need to consider whether the proposed surveillance is no more than necessary to achieve the objective, as the least intrusive method will be considered proportionate by the courts.
- 8.10 The Authorising Officer will also need to take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance. This is known as “**collateral intrusion**”. Measures must be taken whenever practicable to avoid or minimise, so far as practicable, **collateral intrusion**.
- 8.11 When authorising the conduct or use of a **CHIS** the Authorising Officer must also be satisfied that appropriate arrangements are in place for the management and oversight of the **CHIS**. This must address health and safety issues through a risk assessment. The Authorising Officer must also have regard to any adverse impact on community confidence that may result from the use or conduct of the information obtained.
- 8.12 The authorisation does not take effect until a Justice of the Peace has made an order approving the grant of the authorisation.

### Stage 3 - Judicial Approval

- 8.13 If the Authorising Officer is satisfied that the surveillance is *necessary and proportionate*, they will instruct Legal Services to seek approval from a Justice of the Peace sitting at the Magistrates’ Court.
- 8.14 Legal Services will request a hearing date from the Court. The time taken to obtain a hearing date from the Court will need to be taken into account when scheduling any proposed surveillance.
- 8.15 Urgent approvals should not be necessary.
- 8.16 If the approval is urgent and cannot be handled the next working day then the applicant officer should:
  - 8.16.1 phone the Court’s out of hours legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why the police cannot authorise the application.
  - 8.16.2 If urgency is agreed, then arrangements will be made for a suitable Magistrate to consider the application. You will be told where to attend and give evidence.
  - 8.16.3 Attend the hearing as directed with two copies of the signed RIPA authorisation form.
- 8.17 At the hearing the Council will provide the Court with a copy of the authorisation signed by the Authorising Officer, together with any supporting documents relevant to the matter showing the necessity and proportionality of the authorisation and which contain all the information relied upon. Also included will be a summary of the circumstances of the case.
- 8.18 The hearing will be in private heard by a single Justice of the Peace (Magistrate / District Judge) who will read and consider the application.
- 8.19 On reviewing the papers and hearing the application the Justice of the Peace will determine whether they are satisfied that there were, at the time the authorisation was granted, and continue to be reasonable grounds for believing that the authorisation is

*necessary and proportionate*. In addition they must also be satisfied that the Authorising Officer had the relevant authority to authorise the Council's own internal authorisation prior to it passing to the Court.

- 8.20 For authorisations for the use of a **CHIS** the Justice of the Peace will also need to be satisfied that there were and are reasonable grounds for believing appropriate arrangements are in place for the management and oversight of the **CHIS**.
- 8.21 The Justice of the Peace may ask questions of the Council in order to satisfy themselves of the necessity and proportionality of the request.
- 8.22 In considering the application the Justice of the Peace may decide to:
  - 8.22.1 grant an Order approving the authorisation or renewal. The authorisation or renewal will then take effect and the Local Authority may proceed to use surveillance in accordance with the authorisation;
  - 8.22.2 refuse to approve the authorisation or renewal. The RIPA authorisation will not take effect and the Local Authority may not use the proposed surveillance. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the need to go through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those errors have been remedied;
  - 8.22.3 refuse to approve the grant or renewal and quash the authorisation or notice. A Justice of the Peace must not exercise its power to quash an authorisation unless the applicant (the Council) has had at least two business days' notice from the date of the refusal in which to make representations.

#### Stage 4 - Duration and Review

- 8.23 If the Justice of the Peace approves the authorisation, the authorisation will last, in the case of **directed surveillance**, a period of 3 months and, in the case of a **CHIS**, a period of 12 months.
- 8.24 Authorising Officers must then conduct regular reviews of authorisations granted in order to assess the need for the surveillance to continue. Reviews should be conducted on a monthly basis as a minimum. The Authorising Officer may decide that reviews should be conducted more frequently, particularly where a high level of collateral intrusion is likely.
- 8.25 A review involves consultation with the applicant officer and any other persons involved in the surveillance. The applicant officer must give sufficient information about the surveillance and any information obtained by the surveillance for the Authorising Officer to be satisfied that the authorised surveillance should continue. Applicant officers should be pro-active in preparing reports to assist Authorising Officers carry out reviews.

#### Stage 5 - Renewals

- 8.26 If it appears that the surveillance will continue to be *necessary* and *proportionate* beyond the 3 month period for **directed surveillance** or 12 months for use of a **CHIS**, the authorisation must be renewed.
- 8.27 An application for renewal should be made by the applicant officer by completing the appropriate form which is available from the Home Office website (<https://www.gov.uk/government/collections/ripa-forms--2>). This form should then be submitted to the Authorising Officer who must then consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.
- 8.28 The Authorising Officer must be satisfied that it is *necessary* and *proportionate* for the authorisation to continue and that the **Crime Threshold** continues to be met. The authorisation for renewal must then be approved by a Justice of the Peace for it to take effect.
- 8.29 An authorisation may be renewed and approved before the initial authorisation ceases to have effect but the renewal takes effect from the time at which the authorisation would have expired. If necessary, a renewal can be granted more than once.

#### Stage 6 - Cancellations

- 8.30 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting (or renewing) no longer apply or if the authorisation is no longer *necessary* or *proportionate*.
- 8.31 An authorisation can be cancelled on the initiative of the Authorising Officer following a periodic review or after receiving an application for cancellation from the applicant officer. Forms for the cancellation of **directed surveillance** and use of a **CHIS** are available on the Home Office website

(<https://www.gov.uk/government/collections/ripa-forms--2>)

### **9. COMMUNICATIONS DATA**

- 9.1 The term “**communications data**” includes the “who”, “when”, “where”, and “how” of a communication but not the content i.e. what was said or written. It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.
- 9.2 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or e-mail address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.
- 9.3 The acquisition of **communications data** is permitted under Part 3 of the IPA and will be a justifiable interference with an individual’s human rights under the European Convention on Human Rights only if the conduct being authorised or required to take place is *necessary* for the purposes of a specific investigation or operation, *proportionate* and *in accordance with law*.
- 9.4 Training should be made available to all those who participate in the acquisition and disclosure of **communications data**.

- 9.5 The Home Office has published the “Communications Data Code of Practice” (latest edition at time of writing was November 2018). This code should be readily available to persons involved in the acquisition of **communications data** under the IPA and persons exercising any functions to which this code relates must have regard to the code.
- 9.6 The IPA stipulates that conduct to be authorised must be *necessary* for one or more of the purposes set out in the IPA. For Local Authorities this purpose is “for the applicable crime purpose” which means:
- 9.6.1 where the **communications data** is wholly or partly events data (events data covers information about time-bound events taking place across a telecommunication system at a time interval, for example, information tracing the origin or destination of a communication that is, or has been, in transmission), the purpose of preventing or detecting serious crime; or
- 9.6.2 in any other case, the purpose of preventing or detecting crime or of preventing disorder.
- 9.7 “Serious Crime” means:
- 9.7.1 an offence for which an adult is capable of being sentenced to one year or more in prison;
- 9.7.2 any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- 9.7.3 any offence committed by a body corporate;
- 9.7.4 any offence which involves the sending of a communication or a breach of privacy; or
- 9.7.5 an offence which involves, as an integral part of it, or the sending of a communication or breach of a person’s privacy.
- 9.8 A Local Authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

## 10. AUTHORISATION PROCESS - COMMUNICATIONS DATA

- 10.1 Acquisition of **communications data** under the IPA involves four roles:
- 10.1.1 The Applicant Officer - The applicant officer is a person involved in conducting or assisting an investigation or operation within a relevant public authority who makes an application in writing or electronically for the acquisition of **communications data**;
- 10.1.2 The Single Point of Contact (SPoC) - The SPoC is an individual trained to facilitate the lawful acquisition of **communications data** and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications operators and postal operators. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier. The Home Office provides authentication services to enable telecommunications operators and postal operators to validate SPoC credentials;

- 10.1.3 The Senior Responsible Officer - Within every relevant public authority there should be a Senior Responsible Officer. The Senior Responsible Officer must be of a senior rank in a public authority. This must be at least the same rank as the designated senior officer specified in Schedule 4 of the IPA. Where no designated senior officer is specified the rank of the senior responsible officer must be agreed with the Home Office; and
- 10.1.4 The Authorising Individual - **Communications data** applications can be authorised by three separate categories of individual depending on the circumstances of the specific case. The Authorising Individual for Local Authorities is the authorising officer in the OCDA. Section 60A of the IPA confers power on the IPC to authorise certain applications for **communications data**. In practice the IPC will delegate these functions to his staff. These staff will sit in a body which is known as the OCDA.
- 10.2 An authorisation provides for persons within a public authority to engage in conduct relating to a postal service or telecommunication system, or to data derived from such a telecommunication system, to obtain **communications data**. The following types of conduct may be authorised:
- 10.2.1 conduct to acquire **communications data** - which may include the public authority obtaining **communications data** themselves or asking any person believed to be in possession of or capable of obtaining the **communications data** to obtain and disclose it; and/or
- 10.2.2 the giving of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

#### Stage 1 - Making an Application

- 10.3 Before public authorities can acquire **communications data**, authorisation must be given by an Authorising Individual. An application for that authorisation must include an explanation of the necessity of the application.
- 10.4 Necessity should be a short explanation of the investigation or operation, the person and the **communications data** and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of **communications data** is necessary for the statutory purpose specified.
- 10.5 When granting an authorisation the authorising individual must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified **communications data** – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.
- 10.6 As well as consideration of the rights of the individual whose data is to be acquired consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation.
- 10.7 The applicant officer will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring **communications data**.

- 10.8 The application should record subsequently whether it was authorised by an authorising individual and when that decision was made. Applications should be retained by the public authority and be accessible to the SPoC.

#### Stage - 2 Consultation with the Single Point of Contact

- 10.9 A SPoC must be consulted on all Local Authority applications before they are authorised.
- 10.10 Amongst other things the SPoC will:
- 10.10.1 assess whether the acquisition of specific **communications data** from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data; and
- 10.10.2 advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators.
- 10.11 The National Anti-Fraud Network ('NAFN') is hosted by Tameside Metropolitan Borough Council.
- 10.12 In accordance with section 73 of the IPA, all Local Authorities who wish to acquire **communications data** under the IPA must be party to a collaboration agreement. In practice this means they will be required to become members of NAFN and use NAFN's shared SPoC services. Applicant officers within Local Authorities are therefore required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the Local Authority ensuring it acts in an informed and lawful manner.
- 10.13 In addition to being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the local authority is aware the application is being made before it is submitted to an authorising officer in OCDA. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations. In this Council the Chief Executive is the Senior Responsible Officer and the officers notified to the NAFN (notified in March 2019) as able to verify applications are the Head of Legal and Commercial Services and the Audit Manager.
- 10.14 NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

#### Stage 3 - Authorisation of Applications

- 10.15 The (OCDA) performs this function on behalf of the IPC. An authorising officer in OCDA can authorise requests from Local Authorities.
- 10.16 The authorising individual is responsible for considering and, where appropriate, authorising an application for **communications data**. It is their responsibility to consider the application and record their considerations at the time, in writing or electronically in order to show that they have understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny. Comments should be tailored to a specific application as this best demonstrates the application has been properly considered.

- 10.17 If the authorising individual believes the acquisition of **communications data** meets the requirements set out in the IPA and is necessary and proportionate in the specific circumstances, an authorisation will be granted. If the authorising individual does not consider the criteria for obtaining the data have been met the application should be rejected and/or referred back to the SPoC and the applicant officer.

#### Stage 4 - Refusal to Grant an Authorisation

- 10.18 Where a request is refused by an authorising officer in OCDA, the public authority has three options:
- 10.18.1 not proceed with the request;
- 10.18.2 resubmit the application with a revised justification and/or a revised course of conduct to acquire **communications data**; or
- 10.18.3 resubmit the application with the same justification and same course of conduct seeking a review of the decision by OCDA. A public authority may only resubmit an application on the same grounds to OCDA where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. OCDA will provide guidance on its process for reviewing such decisions.

#### Stage 5 - Duration of Authorisations and Notices

- 10.19 An authorisation becomes valid on the date upon which the authorisation is granted. It is then valid for a maximum of one month. This means the conduct authorised should have been commenced, which may include the giving of a notice, within that month.
- 10.20 Any notice given under an authorisation remains in force until complied with or until the authorisation under which it was given is cancelled.
- 10.21 All authorisations should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s). Any period should be clearly indicated in the authorisation. The start date and end date should be given, and where a precise start and end time are relevant these must be specified.
- 10.22 Where an authorisation relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted.
- 10.23 Authorising individuals should specify the shortest possible period of time for any authorisation. To do otherwise would impact on the proportionality of the authorisation and impose an unnecessary burden upon the relevant telecommunications operator(s) or postal operator(s).

#### Stage 6 - Renewal of Authorisations

- 10.24 Any valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation. A renewed authorisation takes effect upon the expiry of the authorisation it is renewing.
- 10.25 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasons for seeking renewal

should be set out by the applicant officer in an addendum to the application upon which the authorisation being renewed was granted.

10.26 Where an authorising individual is granting a further authorisation to renew an earlier authorisation, they should:

10.26.1 consider the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and

10.26.2 record the date and, when appropriate to do so, the time when the authorisation is renewed.

### Stage 7 - Cancellations

10.27 An authorisation may be cancelled at any time by the Local Authority or OCDA and must be cancelled if, at any time after the granting of the authorisation, it is no longer necessary for a statutory purpose or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved.

10.28 In practice, it is likely to be the public authority that is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant officer, where appropriate) must cease the authorised conduct.

10.29 A notice given under an authorisation (and any requirement imposed by a notice) is cancelled if the authorisation is cancelled but is not affected by the authorisation ceasing to have effect at the end of one month period of validity.

## **11. CENTRAL CO-ORDINATION**

11.1 The Chief Executive will be the Senior Responsible Officer for the overall implementation of RIPA and the IPA.

11.2 The Head of Legal and Commercial Services will be responsible for:

11.2.1 giving advice and assistance to all staff concerned with the operation of RIPA and the IPA;

11.2.2 arranging training for all staff concerned with the operation of RIPA and the IPA; and

11.2.3 maintaining and keeping up to date this corporate policy and procedure.

11.3 The Audit Manager will be responsible for:

11.3.1 maintaining a central and up to date record of all authorisations;

11.3.2 along with the Head of Legal and Commercial Services, giving advice and assistance to all staff concerned with the operation of RIPA and the IPA; and

11.3.3 allocating reference numbers to authorisations.

## **12. WORKING WITH OTHER AGENCIES**



12.1 When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this Council will be responsible for obtaining a RIPA authorisation and therefore this Policy and Procedure must be used. The other agency must then be given explicit instructions on what actions it may undertake and how these actions are to be undertaken.

12.2 When another agency (e.g. Police, HMRC, etc):

12.2.1 wish to use the Council's resources (e.g. CCTV surveillance systems) for RIPA purposes, that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes he or she must obtain a copy of that agency's RIPA form, a copy of which must be passed to the Audit Manager for inclusion on the central register;

12.2.2 wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, the request should normally be granted unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the other agency's activities. Suitable insurance or other appropriate indemnities may need to be sought. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not involved in the RIPA activity of the other agency.

### **13. OTHER SOURCES OF INFORMATION**

13.1 The Home Office has issued Codes of Practice on **directed surveillance, CHISs and communications data**. These Codes of Practice supplement this policy and procedure document and should be used as a source of reference by all officers whose task it is to apply the provisions of RIPA and the IPA and their subordinate legislation.

### **14. RECORDS MANAGEMENT**

14.1 The Council must keep a detailed record of all authorisations, judicial approvals, reviews, renewals, cancellations and rejections in the relevant services. A central record of all authorisation forms, whether authorised or rejected, will be maintained and monitored by the Audit Manager.

14.2 All Authorising Officers must send all original applications for authorisation to the Audit Manager. Each document will be given a unique reference number, the original will be placed on the central record and a copy will be returned to the applicant officer.

14.3 Copies of all other forms used and the judicial approval form must be sent to the Audit Manager bearing the reference number previously given to the application to which it refers.

#### Service Records

14.4 Each service must keep a written record of all authorisations issued to it, and any judicial approvals granted, to include the following:

14.4.1 a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

14.4.2 a record of the period over which the operation has taken place;

- 14.4.3 the frequency of reviews prescribed by the Authorising Officer;
- 14.4.4 a record of the result of each review;
- 14.4.5 a copy of any renewal of an authorisation and any supporting documentation submitted when the renewal was requested;
- 14.4.6 the date and time when any instruction was given by the Authorising Officer, including cancellation of such authorisation;
- 14.4.7 a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace; and
- 14.4.8 the required date of destruction and when this was completed.

Central Record Maintained by the Audit Manager

- 14.5 A central record of all authorisation forms, whether authorised or rejected, is kept by the Audit Manager. The central record must be readily available for inspection on request by the Investigatory Powers Commissioner.
- 14.6 The central record must be updated whenever an authorisation is granted, reviewed, renewed or cancelled. Records will be reviewed after a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive and deleted when no longer necessary.
- 14.7 The central record must contain the following information:
  - 14.7.1 the type of authorisation;
  - 14.7.2 the date on which the authorisation was given;
  - 14.7.3 name / rank of the Authorising Officer;
  - 14.7.4 details of attendances at the Magistrates' Court to include date of attendances at court, the determining Justice of the Peace, the decision of the Justice of the Peace and the time and date of that decision;
  - 14.7.5 the unique reference number (URN) of the investigation / operation. This will be issued by the Audit Manager when a new application is entered in the Central Record. The applicant officer will be informed accordingly and should use the same URN when requesting a renewal or cancellation;
  - 14.7.6 the title of the investigation / operation, including a brief description and names of the subjects, if known;
  - 14.7.7 if the authorisation was renewed, when it was renewed and who authorised the renewal, including the name and rank / grade of the Authorising Officer;
  - 14.7.8 whether the investigation / operation is likely to result in the obtaining of **confidential information** (information is confidential if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, information from a patient's medical records; or matters subject to legal privilege);

- 14.7.9 if the authorisation was reviewed, when it was reviewed and who authorised the review, including the name and rank / grade of the Authorising Officer;
- 14.7.10 the date and time that the authorisation was cancelled.
- 14.8 It should also contain a comments section enabling oversight remarks to be included for analytical purposes.
- 14.9 The Audit Manager co-ordinating RIPA and IPA applications ensures that there is an awareness of the investigations taking place. This would also serve to highlight any unauthorised **covert** surveillance being conducted.

#### Retention and Destruction of Material

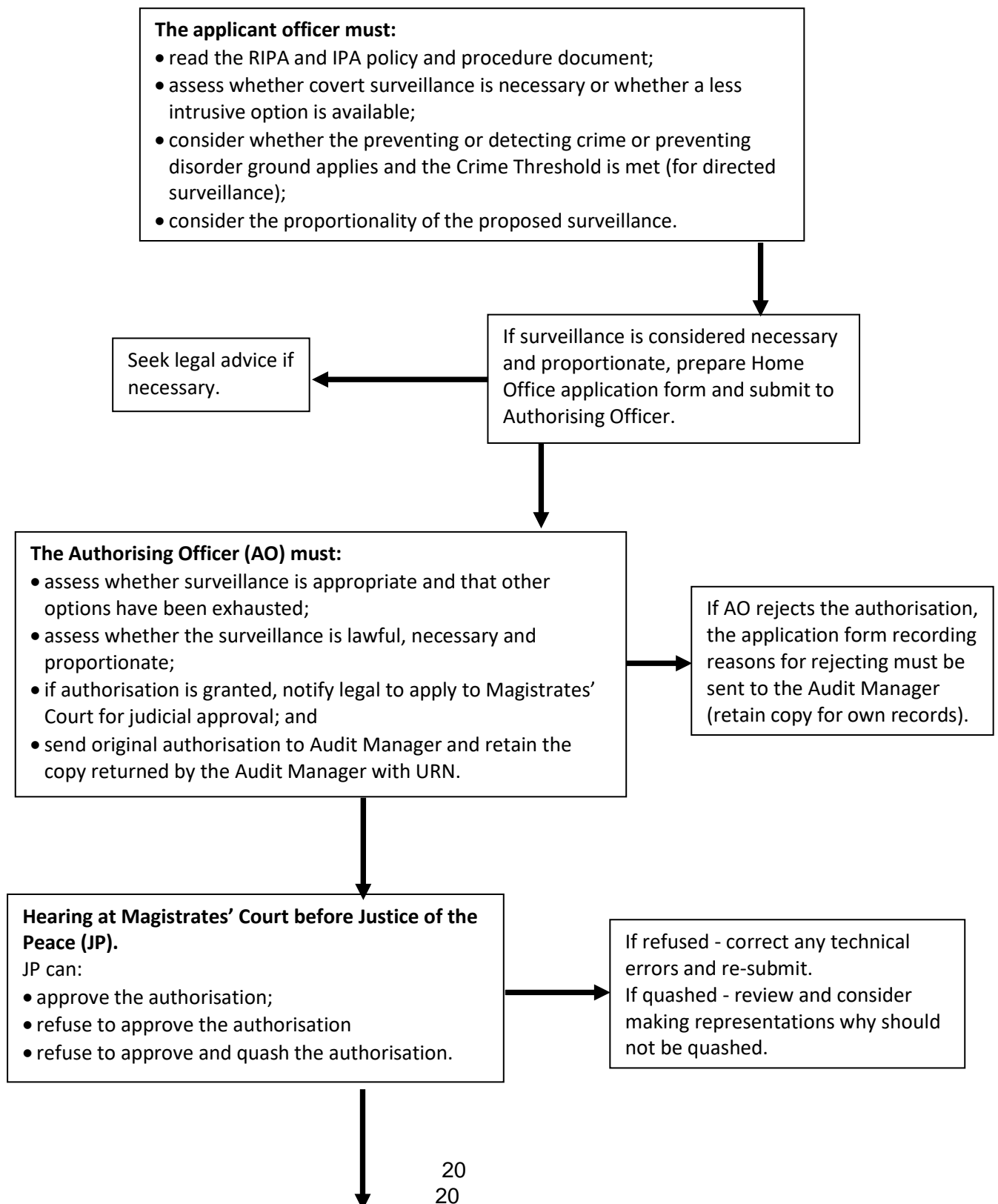
- 14.10 Departments must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of **covert** surveillance, a CHIS and/or the acquisition of communications data which accord with the Council's Information Management Policy. Records will be reviewed after a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive and must be destroyed as soon as they are no longer necessary. **Confidential material must be destroyed as soon as it is no longer necessary.** It must not be retained or copied unless it is necessary for a specified purpose. Where there is doubt, advice must be sought from the Head of Legal and Commercial Services or the Senior Responsible Officer.

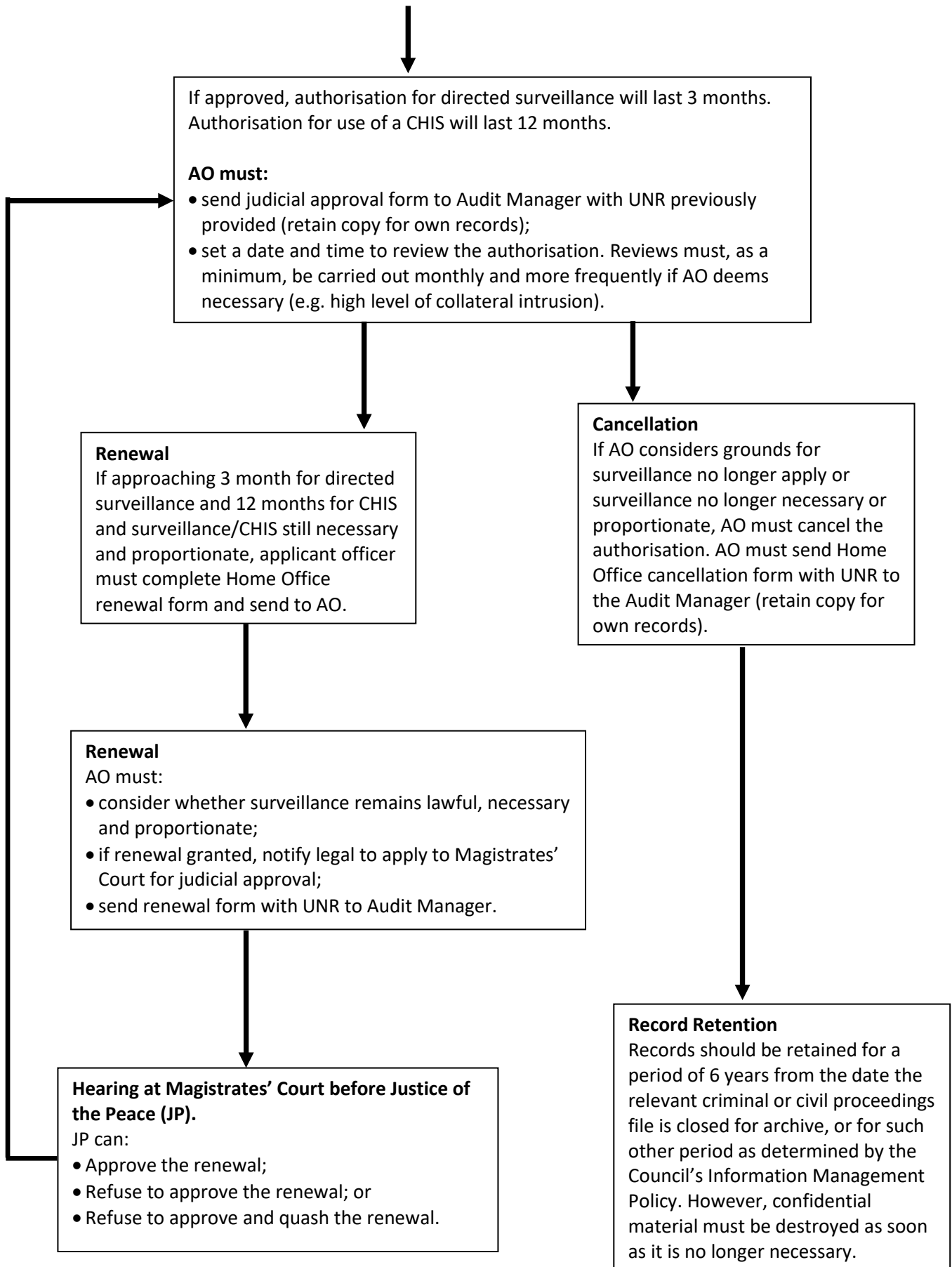
## 15. REVISION HISTORY

Date	Action
December 2006	ASG Revised
May 2009	ASG Reviewed
June 2010	AW Reviewed and updated
March 2012	ASG Revised
October 2012	HO Guidance issued
September 2013	RH Reviewed and updated
October 2015	DMG Reviewed and updated
9 December 2015	Approved by Audit and Governance Committee
12 January 2016	Approved by Council

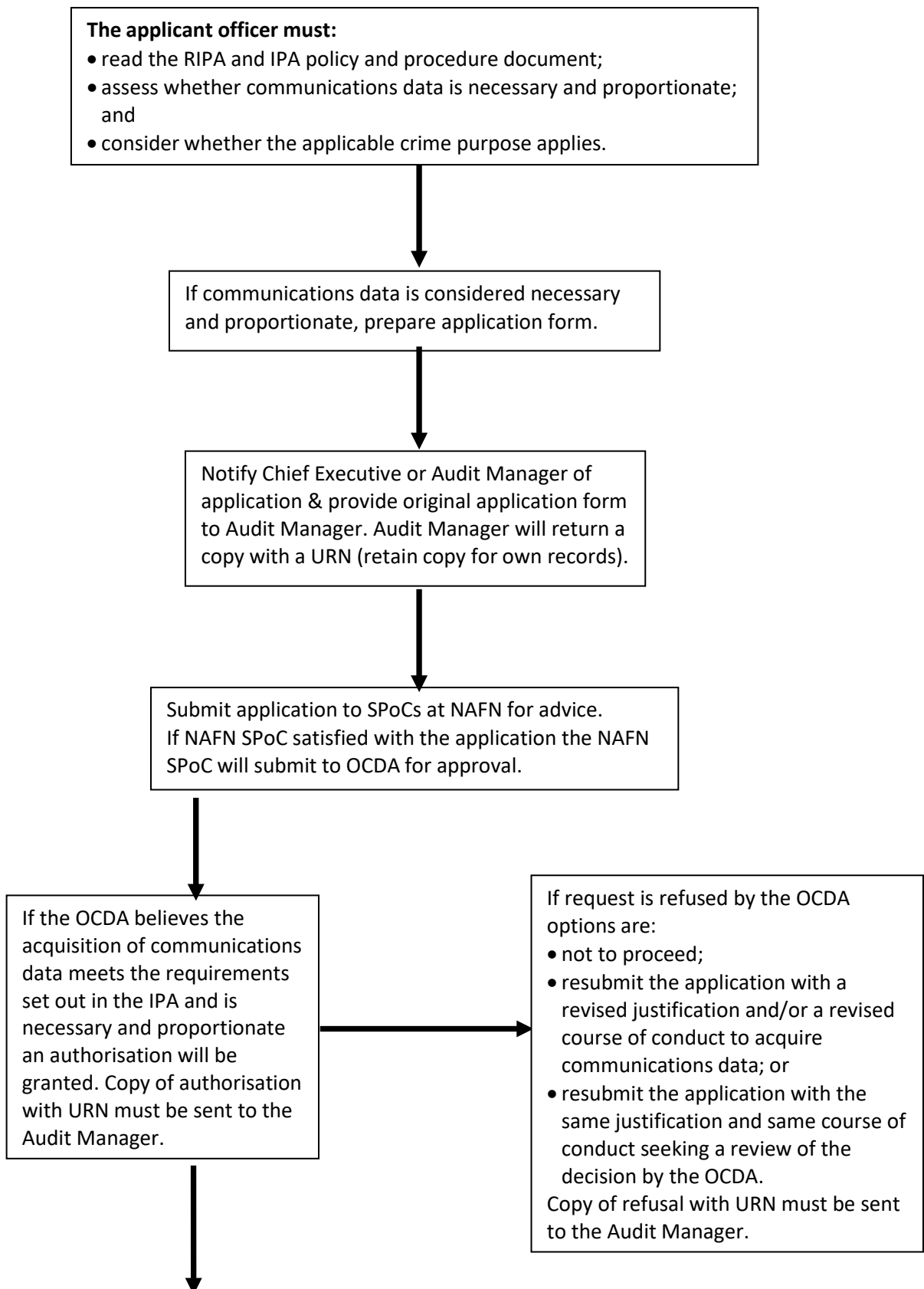
**RIPA - AUTHORISATION OF DIRECTED SURVEILLANCE / USE OF A CHIS PROCEDURE**

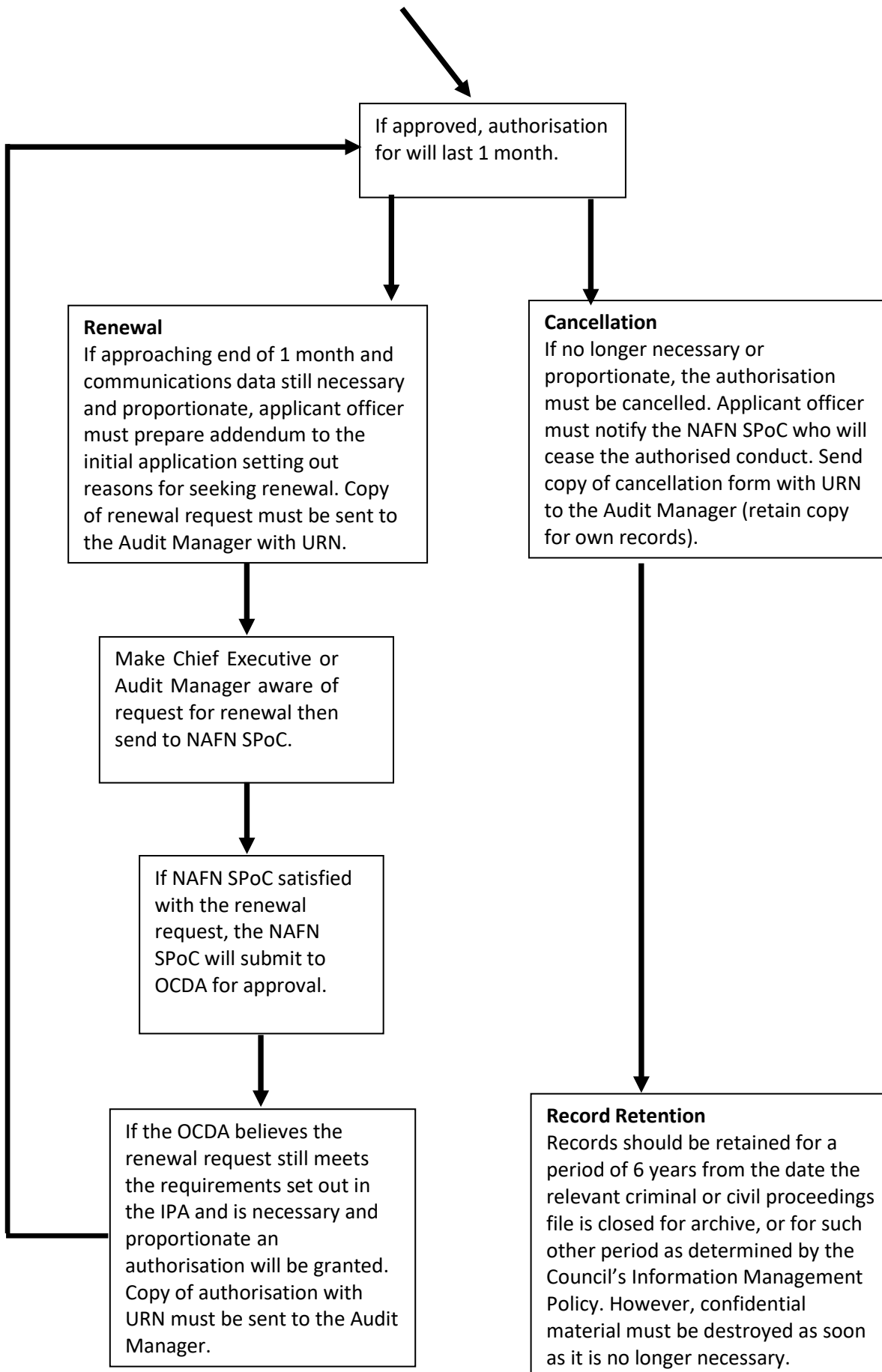
(Note: Note: Only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS)





**IPA - COMMUNICATIONS DATA AUTHORISATION PROCESS**





This page is intentionally left blank