CYNGOR SIR CEREDIGION

CEREDIGION COUNTY COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 ('RIPA') PART II

Directed Surveillance, Covert Human Intelligence Sources and Communications Data

CORPORATE POLICY & PROCEDURES DOCUMENT

- **Adopted by Council 5th March 2020**
- **Revised by SRO July 2021**

INDEX

CEREDIGION COUNTY COUNCIL
COVERT SURVEILLANCE - POLICY STATEMENT

Introduction

1. Ceredigion County Council ('the Council') is committed to building a fair and safe community for all by ensuring the effectiveness of laws designed to protect individuals, businesses, the environment and public resources.

2. The Council recognises that most organisations and individuals appreciate the importance of these laws and abide by them. The Council will use its best endeavours to help them meet their legal obligations without unnecessary expense and bureaucracy.

3. At the same time, the Council has a legal responsibility to ensure that those who seek to flout the law are the subject of firm but fair enforcement action. Before taking such action, the Council may need to undertake covert surveillance of individuals and/or premises to gather evidence of illegal activity.

Procedure

4. All covert surveillance shall be undertaken in accordance with the procedures set out in this document.

5. Ceredigion County Council shall ensure that covert surveillance is only undertaken where it complies fully with all applicable laws; in particular the:

   - The Human Rights Act 1998;
   - The Regulation of Investigatory Powers Act 2000 ('RIPA');
   - Protection of Freedoms Act 2012;
   - The Investigatory Powers Act 2016 ('IPA 2016'); and
   - The Data Protection Act 2018.

6. The Council shall, in addition, have due regard to all secondary legislation (including Regulations and orders), official guidance and codes of practice, particularly those issued by the Home Office, the Office of the Surveillance Commissioners ('OSC'), the Security Camera Commissioner and the Information Commissioner.

7. In particular, the following guiding principles shall form the basis of all covert surveillance activity undertaken by the Council:

   - Covert surveillance shall only be undertaken where it is absolutely necessary to achieve the desired aims;
   - Covert surveillance shall only be undertaken where it is proportionate to do so and in a manner that it is proportionate;
   - Adequate regard shall be had to the rights and freedoms of those who are not the target of the covert surveillance;
   - All authorisations to carry our covert surveillance shall be granted by appropriately trained and designated Authorising Officers; and
   - Covert surveillance (regulated by The Regulation of Investigatory Powers Act 2000 ('RIPA') shall only be undertaken after obtaining judicial approval.

Training and Review

8. All Council officers undertaking covert surveillance shall be appropriately trained to ensure that they understand their legal and operational obligations. Officers should be competent and confident in the RIPA roles they perform. Refresher training should be provided and undertaken as necessary, to include practical exercises and account taken of any legislative changes. Training should also include guidance on completion of application forms.

9. Regular audits shall be carried out to ensure that Officers are complying with this policy.

10. This policy should be reviewed at least once a year, to ensure it remains fit for purpose.

11. The operation of the Council's RIPA activity shall be overseen and monitored by the Council's Overview and Scrutiny Co-ordinating Committee, by receiving reports every six months.

Conclusion

12. All citizens will reap the benefits of this Policy, through effective enforcement of criminal and regulatory legislation and the protection that it provides.

13. Adherence to this Policy will minimise intrusion into citizens' lives and will avoid any legal challenge to the Council's covert surveillance activities.

14. Any questions relating to this policy should be addressed to the Corporate Lead Officer-Legal & Governance (Monitoring Officer & Senior Responsible Officer).

Date ……..

PART 1 – INTRODUCTION TO SURVEILLANCE REGULATED BY CHAPTER 2 OF RIPA

The Regulation of Investigatory Powers Act 2000 ('RIPA') regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

Ceredigion County Council ('the Council') is therefore included within the legislative framework with regard to the authorisation of directed surveillance, the use of covert human intelligence sources and accessing communications data.

Some sections of RIPA have been repealed and replaced by the Investigatory Powers Act 2016 ('IPA 2016'). As well as RIPA itself, several sets of Regulations have been produced along with three Home Office Codes of Practice.

The Council has had regard to the Codes of Practice produced by the Home Office, the procedures and guidance produced by Office of Surveillance Commissioners and Codes of Practice issued by the Information Commissioners in preparing this guidance and each Department should hold copies to which staff can refer.

Objectives of this document

The objective of this document is to ensure that all covert surveillance (as defined by RIPA and associated legislation and guidance) conducted by Council Officers is carried out appropriately and on a lawful basis. This document should be read in conjunction with the Home Office Revised Code of Practice on Covert Surveillance and Property Interference 2018, Covert Human Intelligence Sources, Camera Code of Practice and the Investigatory Powers Commissioner's Office (formerly Office of Surveillance Commissioners) Procedures and Guidance. Schedule 1 (below) lists current legislation and guidance that must be read in conjunction with this document, but this list is not exhaustive.

If the procedures outlined in this Policy are not followed, any evidence acquired as a result of surveillance activities may be susceptible to a human rights challenge. It may therefore not be admissible in Court, and the Council is unlikely to take proceedings based on such evidence. The Council may also be exposed to legal action by individuals who claim that their human rights to privacy and respect for family life will have been abused. See 'Dealing with complaints from the public' below.

Scope of this document

This document explains the Council's statutory responsibility to comply with RIPA, and associated legislation. It provides guidance and sets out the Council's procedures and matters to consider in relation to the following:

- Directed surveillance – see Part 2 below;
- A Covert Human Intelligence Source ('CHIS') – see Part 3 below; and
- Acquisition of Communications Data (through NAFN's SPOC) – see Part 5 below.

Parts 1 - 3 of this Policy only apply where surveillance is covert and directed i.e. where the individual or individuals are not aware at the time of surveillance that surveillance is being carried out. The purpose of these parts are to help officers decide what type of surveillance they are undertaking, whether it is regulated by Chapter 2 of RIPA, confirm the relevant procedures and provide guidance.

Part 4 deals with the keeping of records, data handling, retention safeguards & dealing with complaints and errors.

Separate non-RIPA guidance is also set out (see Part 6 below) below for observations or surveillance which are not carried out covertly.

The Information Commissioner has issued a separate Code of practice on the use of CCTV surveillance (available at: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf).

Ceredigion County Council's statutory responsibility

The Council has a statutory responsibility to comply with the Human Rights Act 1998, which contains the Articles and Protocols of the European Convention for the Protection of Human Rights ('ECHR') that are deemed to apply in the UK. Since the UK's withdrawal from the European Union, a review is being undertaken in relation to the Human Rights Act 1998 but it currently remains in force.

Section 6 of the Human Rights Act 1998 makes it unlawful for the Council to act in any way that is incompatible with the ECHR.

Article 8 ECHR provides that:

- Everyone has the right to respect for his private and family life, his home and his correspondence; and
- There shall be no interference by a public authority with the exercise of this right except such as is:
    a) In accordance with the law; and
    b) Necessary in a democratic society in the interests of public safety, prevention of disorder or crime, protection of health or morals and protection of the rights and freedoms of others.

Therefore, surveillance will breach a person's human rights unless it is authorised under RIPA. RIPA provides the legal framework for lawful interference.

Obtaining authorisation to conduct surveillance in accordance with RIPA helps to protect the Council and its officers from complaints of interference with the rights protected by Article 6 and Article 8(1) ECHR, which is now enshrined in English law through the Human Rights Act 1998. This is to ensure any interference with the private life of citizens will be '*in accordance with the law'*.

Provided activities undertaken are also '*necessary and proportionate'* (see subsequent parts in this document for further details) they will not be in contravention of Human Rights legislation.

Information is considered private information if it includes any information relating to the subject's private or family life or the private or family life of any other person. It would include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Private information may include personal data, for example, names, telephone numbers and address details.

For example, where two people hold a conversation on the street they may have a reasonable expectation of privacy over the contents of that conversation. However, a directed surveillance authorisation may be required if a public authority's records or listens to the conversation as part of a specific investigation or operation.

Therefore, '*private information'* may be acquired through authorised covert directed surveillance even where a person is in a public place and may have a reduced expectation of privacy.

Furthermore, information relating to the private life of an individual may be obtained when a number of records are analysed together, or where a number of pieces of information are obtained, covertly, for the purpose of making a record about a person or for data processing to generate further information.

The totality of the information may constitute private information even if the individual records do not. For example, enforcement officers may photograph the exterior of business premises for record purposes without the need for a RIPA authorisation. If, however, the officers wished to establish a pattern of occupancy of those premises by any person and took photographs on a number of occasions, that conduct would likely to result in the obtaining of private information and thus compliance with RIPA would be required.

The role of Elected Members

The statutory Codes of Practice issued pursuant to RIPA, namely the revised Covert Surveillance and Property Interference Code Practice 2018, states that elected Members should review the Council's use of RIPA and set the Policy at least once a year.

Members should also consider internal reports on the use of RIPA on a regular basis to ensure that it is being used consistently with the Council's policy and that the policy remains fit for purpose.

The role of the Senior Responsible Officer ('SRO')

The statutory Codes of Practice issued pursuant to RIPA, namely the revised Covert Surveillance and Property Interference Code of Practice 2018 considers that councils should appoint an SRO.

Ceredigion County Council's SRO is the Corporate Lead Officer-Legal & Governance/ Monitoring Officer. The SRO should be able to advise Officers on the RIPA procedure and be responsible for:

1. The integrity of the process in place within the public authority to authorise directed surveillance, the use of covert human intelligent sources and interference with property or wireless telegraphy;

2. Compliance with Chapter 2 of RIPA and with the relevant codes; and

3. Engagement with the Commissioners and inspectors when they conduct their inspections, and where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.

In addition, the SRO will be responsible for overseeing and co-ordinating:

1. The submission of quarterly reports detailing RIPA activity, to the Overview and Scrutiny Co-ordinating Committee;

2. The annual review by the Overview and Scrutiny Co-ordinating Committee of this Policy;

3. The identification of issues in the oversight process, to enable analysis of issues, evidencing results, and ensuring subsequent feedback into the RIPA training, to ensure these matters are corporately addressed;

4. The formal oversight of the RIPA process within the Council, including identifying individual and corporate training needs, and dissemination of information; and

5. Maintaining online persona/pseudonyms Register including details of services/individuals who can use/sanction them.

The role of the Investigatory Powers Commissioner's Office ('IPCO')

The IPA 2016 provides for an Investigatory Powers Commissioner ('*the Commissioner*'), whose remit includes providing comprehensive oversight of the use of the powers to which this code applies, and adherence to the practices and processes described in it.

The IPCO acts as the regulatory body in respect of the Directed Surveillance, Covert Human Intelligence Source aspects of RIPA and Communications Data. This Office conducts inspections of local authorities to ensure they are compliant with RIPA insofar as authorisations for directed surveillance and use of covert human intelligence sources is concerned. The IPCO does not give legal advice, although guidance may be given, when appropriate to request originating from the Senior Responsible Officer of a public authority.

Further information about the Investigatory Powers Commissioner, their office and their work may be found at: www.ipco.org.uk.

The role of the Information Commissioners Office ('ICO')

The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting good practice, openness by public bodies, data privacy for individuals and providing advice on standards. Audits also look at the way organisations handle requests for information under the Freedom of Information Act 2000.

PART 2 – DIRECTED SURVEILLANCE

Chapter 2 of RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities to ensure that they are compatible with the ECHR, particularly Article 8 (the right to respect for private and family life).

The first issue for any local authority officer who is considering undertaking covert surveillance is what type of surveillance they are undertaking, and **whether it is something that can be authorised under RIPA.** Directed Surveillance is one of the two surveillance techniques available to the Council under Part 2 of Chapter 2 of RIPA. The second available technique is a CHIS, but the third, Intrusive Surveillance, cannot be authorised by the Council.

The Covert Surveillance and Property Interference Revised Code of Practice 2018 confirms at paragraph 2.2 and 2.3 that:

'*Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained*

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.'

Meaning of 'Directed Surveillance'

Directed Surveillance is defined in S.26 (2) of RIPA:

'Subject to subsection (6), surveillance is directed for the purposes of this Part if it is covert but not intrusive and is undertaken –

(a) for the purposes of a specific investigation or a specific operation;
(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.'

Typically, local authorities may use Directed Surveillance when investigating benefit fraud, trading standards offences or antisocial behaviour. This may involve covertly filming or following an individual or monitoring their activity in other ways.

Before undertaking any covert surveillance activity, an investigating officer must ask (and have an affirmative answer to) five questions before the activity can be classed as Directed Surveillance:

- Is the surveillance, actually 'surveillance' as defined by RIPA?
- Will it be done covertly?
- Is it for a specific investigation or a specific operation?
- Is it likely to result in the obtaining of private information about a person?
- Will it be done, otherwise than in an immediate response to events?

See ***Flowchart 1 below*** *to assess when deciding if surveillance is directed.*

Key Points to Note:

A. **General observations** do not constitute Directed Surveillance. The revised Covert Surveillance and Property Interference Code of Practice 2018 (at Paragraph 3.33) states:

> *'The general observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation'*

B. Surveillance is only directed if it is **covert**. The revised Covert Surveillance and Property Interference Code of Practice 2018 (at Paragraph 2.3) states (per 26(9)(a) RIPA):

> *'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'*
>
> This requires investigating officers to consider the manner in which the surveillance is going to be undertaken. If it is done openly, without making any attempt to conceal it or a warning letter is served on the target before the surveillance is done, then it will not be covert.

C. The definition of '***private information***' is very wide. The revised Covert Surveillance and Property Interference Revised Code of Practice 2018 states:

> *'3.3 The 2000 Act states that 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. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.*
>
> *3.4 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites'*
>
> There is a common misconception that if investigating officers are watching someone covertly in a public place or observing activities in an office or business premises that

there is no private information likely to be obtained and so there is no Directed Surveillance. The above sections of the code make it extremely unlikely that a public authority will be able to successfully argue that surveillance will never result in private information being obtained.

D. Where covert surveillance needs to be done in an **emergency** and there is no time to authorise the activity (i.e. an urgent response to events), the surveillance can still be done but it will not require Directed Surveillance authorisation. Nonetheless, it is important to note that it would be very unlikely that these circumstances would apply to the Council, as, if challenged, the Council would be required to demonstrate that it was an immediate response to events and not reasonably practicable for the authorisation to be sought. This course of action is not recommended and if it is considered that there is an emergency situation, advice from the SRO should be sought immediately.

The revised Covert Surveillance and Property Interference Revised Code of Practice 2018 (at Paragraph 3.32) states:

'Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under the 2000 Act, would not require a directed surveillance authorisation. The 2000 Act is not intended to prevent law enforcement officers fulfilling their legislative functions. To this end section 26(2)(c) of the 2000 Act provides that surveillance is not directed surveillance when it is carried out by way of an immediate response to events or circumstances the nature of which is such that it is not reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.'

The Covert Surveillance and Property Interference Revised Code of Practice 2018 gives the example of an authorisation under RIPA not being appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol or monitor social media accounts during a public order incident.

E. Online Covert Activity

The Council's RIPA Social Media Policy (available at [enter link]) sets out what the Revised Covert Surveillance and Property Interference Code of Practice states regarding online covert activity, and its relevant advice to assist Officers in understanding when a RIPA authorisation may be required. See the Council's RIPA Social Media Policy for the Council's requirements and guidance regarding on-line personas.

The Covert Surveillance and Property Interference Revised Code of Practice 2018 (at Paragraph 3.10) states that:

"The growth of the internet and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisations; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations

may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate".

Paragraphs 3.11 – 3.17 of the Code also contain relevant advice and will assist Officers in understanding when a RIPA authorisation may be required:-

3.11 *"The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).*

3.12 *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 a public authority has 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.*

3.13 As set out in paragraph 3.14 below, 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.

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, 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.

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's 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 a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6.

Example 1: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 2: *A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

Example 3: *A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

3.16 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 organisation;

Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);

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 private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.17 Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

Example: *Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered."*

Any systematic, repeated viewing of an individual's online presence, covertly, and which may engage privacy considerations, requires the consideration of a RIPA authorisation.

In accordance with para 4.16 of the Covert Surveillance and Property Interference Code of Practice, where a public authority intends to access a social media or other online account to which they have been given access with the consent of the owner, the Authority will still need to consider whether the account may contain information about others who have not given their consent and if so the need for a directed surveillance authorisation should be considered.

Where several agencies are working together, only one of them would need to obtain an authorisation for covert activity were that deemed to be necessary and proportionate in the circumstances.

On-line personas

Where these are permitted to be used corporately, the SRO will maintain a central register of these pseudonyms, profiles/accounts, together with details of the services or individual officers permitted to use/sanction their use.

Covert Surveillance Social Media & On-line Persona Information

Relevant Council Services are required to:

- record information/data relating to covert social media/on-line surveillance, including on-line personas (* see below)
- identify a Designated Officer
- provide this data to the Designated Officer; and
- the Designated Officer must provide the information to the SRO or the SRO's Representative (Governance Officer) every 4 months.

*The Designated Officer will be required to maintain the following information:

- which media sites/on-line profiles have been visited
- was access to the media site(s)/on-line profile(s) restricted (provide details);
- when were the media site(s)/on-line profile(s) visited;
- by whom (Officer/User);
- on whose request;
- who authorised;
- details of the surveillance e.g. case reference, operation, investigation;

- date of request;
- date of access;
- on which profile/social media account;
- was an on-line persona/false profile/false identity used? If so, which?
- was an official corporate profile used? If so, which?
- how many viewings;
- length of viewing(s);
- for what purpose/rationale was the media site(s)/on-line profile(s) visited;
- Confirmation that the person whose identity is used has explicitly consented in writing, and their protection considered, and details of what is/is not to be done;
- Aim/desired information;
- was the subject aware;
- what data was obtained (including collateral information);
- what was done with any resultant product;
- Details of Social Media relevant to Application;
- Explanation why on-line persona required and alternative methods considered;
- Confirmation as to whether a Risk Assessment has been considered/carried out; and
- Any result, including any risk to Officer (and if not, why not).

Officers who use such sites must also adhere to the Corporate Social Media policy (2016) (available on the Council's intranet site (CeriNet).

- '*5.6 During work time employees may only access and view pages from allowed social media sites which are required in their role.*

- *Use of sites must be justifiable and approved by their line manager in advance of accessing such sites.*

- *6.3 Staff in a safeguarding environment must recognise the sensitivity inherent in their roles and before engaging in any social media activity they should consider if their actions could create any potential safeguarding concerns*

- *Ensure that your personal Facebook account does not compromise your professional position you should ensure that your privacy settings are set correctly*

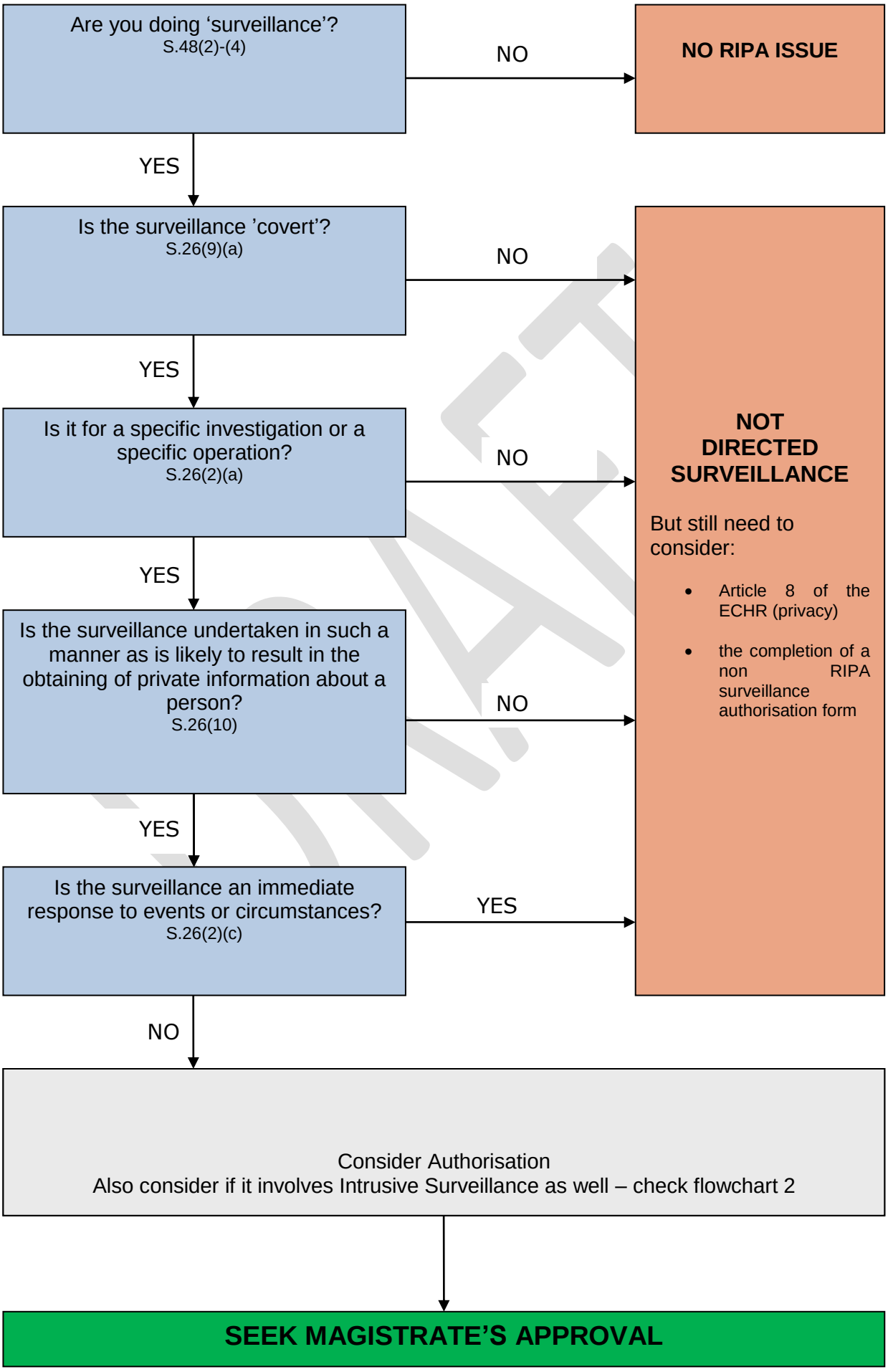
- *Do not use your work contact details as part of your personal profile*
- *Do not use your personal profile in any way for official Council business.*

- *On your personal profile-Do not accept friend requests from members of the public where the primary relationship is through your work.*

- *On your personal profile-Do not accept friend requests from pupils (or their parents) or vulnerable adult service users that you work with.*'

The Council's RIPA Social Media Policy applies to all Council employees and sets out the position of the Council regarding the use of the internet, mobile web browsing and specifically social media websites, when undertaking surveillance, which could include an investigation, in accordance with RIPA. The Council's RIPA Social Media Policy should be read in conjunction with this document.

Flowchart 1 – Are you conducting 'Directed Surveillance'?



Meaning of 'Intrusive Surveillance'

S.26 (3) RIPA states:

> *'Subject to subsections (4) to (6), surveillance is intrusive for the purposes of this Part if, and only if, it is covert surveillance that—*
> *(a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and*
> *(b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.'*

As the name suggests, this type of surveillance is much more intrusive and so the legislation is framed in a way as to give greater protection to the citizen when it is used. Applications to carry out Intrusive Surveillance can only be made by the senior Authorising Officer of those public authorities listed in or added to S.32(6) of RIPA or by a member or official of those public authorities listed in or added to section 41(l). Local authorities **cannot authorise intrusive surveillance.**

It is still important to understand the definition of Intrusive Surveillance because sometimes over-zealous officers may overstep the mark and end up doing it. The following questions have to be asked:

- Is it Covert Surveillance as defined by RIPA?
- Is it being carried out in relation to anything taking place on any residential premises or in any private vehicle?
- Does it involve the presence of an individual on the premises or in the vehicle? and
- Is it being carried out by means of a surveillance device on the premises or in the vehicle?

See Flowchart 2 *to assess if the surveillance is Intrusive.*

Key Points to Note:

A. When doing covert surveillance of premises it can only be 'intrusive' if it is carried out in relation to anything taking place on residential premises. This is defined in S.48(1) RIPA:

   'residential premises" means (subject to subsection (7)(b)) so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used);'

   Covert surveillance of business premises will not be regarded as intrusive surveillance, e.g. where an officer is conducting surveillance of a unit on an industrial estate where a food business is suspected of producing counterfeit vodka, or a retail shop suspected of selling tobacco to under 18's, etc.

   However, care must be taken where a business is located within a building or vehicle, which is also used as a private dwelling, e.g. a person, suspected of manufacturing counterfeit DVDs from a caravan that is also their private residence. No surveillance (which includes filming or capturing images) of persons and activities within those private living quarters is permitted as this would be considered as intrusive surveillance.

B. Not all surveillance of vehicles is 'intrusive'; the target has to be a private vehicle as defined in S.48(1):

'private vehicle" means (subject to subsection (7)(a)) any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it;'

The vehicle can be owned, borrowed, rented or leased. However (by virtue of S.48 (7) (a)) surveillance is not Intrusive where the target vehicle is a taxi or a chauffeur-driven vehicle such as a public coach service.

C. For the surveillance to be intrusive rather than directed it has to be undertaken in such a manner as to involve the presence of an individual on the premises or inside the vehicle.

It is extremely unlikely that local authorities would allow their staff to undertake surveillance by getting inside a private vehicle covertly. However, it may be that an officer is stationed inside residential premises to covertly observe anti-social behaviour.

Whilst normally this kind of conduct is the realm of the police, care must be taken. For example, a keen investigator taking covert pictures from outside a house may decide to move to a more covert position or location to obtain clearer images.

D. Surveillance can still be Intrusive even if the investigating officer is not on or inside the premises or vehicle but is using a surveillance device such a camera, listening device, recorder or even binoculars.

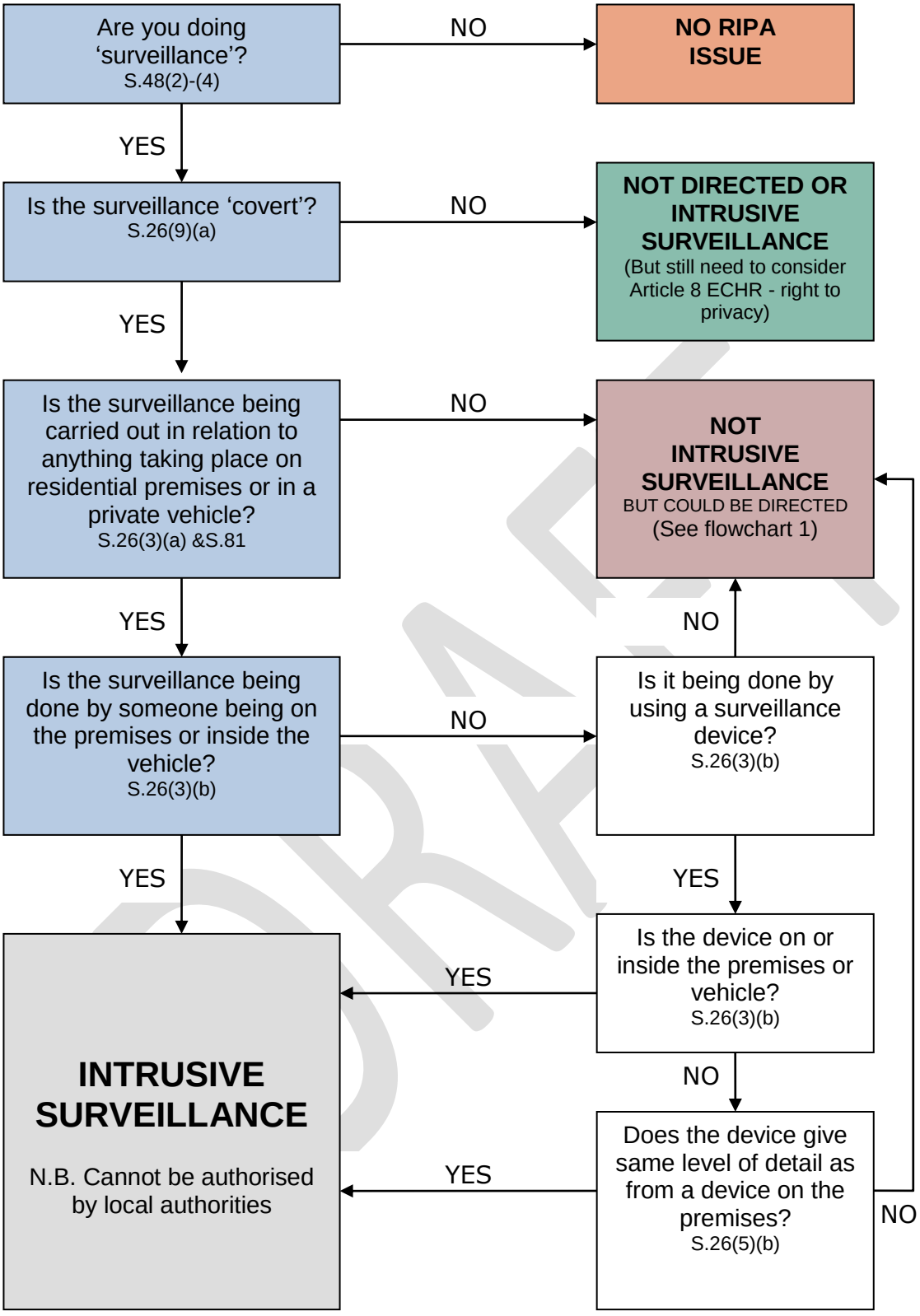
However the words of S.26 (5) should be noted:

'For the purposes of this Part surveillance which –

(a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle, but

(b) is carried out without that device being present on the premises or in the vehicle, is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.'

Flowchart 2 - Are you doing 'Intrusive Surveillance'?



Limitations on the use of Directed Covert Surveillance

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI no. 1500) imposes restrictions on local authorities' use of RIPA (see paragraph 4.44 of the Covert Surveillance and Property Interference Revised Code of Practice 2018).

It restricts AOs in a local authority in England or Wales from authorising the carrying out of directed surveillance unless it is necessary for the purpose of preventing or detecting a criminal offence and meets the following conditions:

- That the criminal offence to be prevented or detected is punishable by a maximum term of at least six months' imprisonment or
- Constitutes an offence under sections 146, 147 or 147A of Licensing Act 2003 (sale of alcohol to children) or section 7 of the Children and Young Persons Act 1933 (sale of tobacco to children under 18 years old).

This '*crime threshold*' does not apply to the authorisation of local authority use of CHIS or the acquisition of communications data.

The amendments to the legislation continues to allow the Council to authorise use of directed surveillance but only in more serious cases as long as the other tests are met i.e. that it is '*necessary*' and '*proportionate*' and where prior approval from a Justice of the Peace (Magistrate) has been granted.

It is therefore essential that investigating officers consider the penalty attached to the criminal offence, which they are investigating, **BEFORE** considering whether it may be possible to obtain an authorisation for directed surveillance.

If an AO is in any doubt about authorising any surveillance activity, they should seek advice from the SRO.

Enhanced authorisation levels

Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material may be authorised only by AOs entitled to grant authorisations in respect of confidential or privileged information. This type of material includes:

- Material subject to legal privilege;
- Confidential personal information;
- Confidential constitution information; and
- Confidential journalistic material and journalists sources.

In the Council, the AO entitled to grant authorisations in respect of confidential or privileged information is the Chief Executive, or (in their absence) the person acting as the Chief Executive (i.e. Corporate Director).

Care must be taken where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality may be involved.

Where such material has been acquired and retained, the Council's SRO must be informed as soon as possible, as the matter should be reported to the IPCO during their next inspection and the material should be made available to the IPCO, if requested.

Note that RIPA does not enable the Council to make any authorisations to carry out intrusive surveillance (for further details, see Part 2 below).

Urgent cases – (Para 4.42 Covert Surveillance and Property Interference Revised Code of Practice 2018)

Paragraph 4.42 of the Covert Surveillance and Property Interference Revised Code of Practice 2018 states that:

> '*The Protection of Freedoms Act 2012 amended the 2000 Act to make local authority authorisations subject to judicial approval. The change means that local authorities need to obtain an order approving the grant or renewal of an authorisation from a judicial authority, before it can take effect. In England and Wales an application for such an order must be made to a Justice of the Peace (JP). If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he or she will issue an order approving the grant or renewal for the use of the technique as described in the application. The amendment means that* ***local authorities are no longer able to orally authorise the use of RIPA techniques.*** *All 37 The senior responsible officer should be a person holding the office, rank or position of an authorising officer within the relevant public authority.* ***authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained.***'

This means that Local Authorities are not able to verbally authorise the use of RIPA techniques. All authorisations must be made in writing and require judicial approval. The authorisation cannot commence until this has been obtained. The SRO should be a person holding the office, rank or position of an AO within the relevant public authority.

A case is not normally regarded as urgent unless the time that would elapse would, in the opinion of the AO be likely to endanger life or jeopardise the investigation for which the authorisation was being given.

An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or is of the AO's or applicant's own making.

PROCEDURE FOR APPLYING FOR A DIRECTED SURVEILLANCE AUTHORISATION

If a Council Officer believes that their intended actions fall under the definition of directed covert surveillance, they will need to apply for a RIPA directed surveillance authorisation.

The 3 key elements of any RIPA authorisation are **necessity, proportionality** and whether there is any risk of **collateral intrusion.**

Before the Authorising Officer authorises the RIPA application, they will need to be sure that the authorisation is **necessary** for the purpose of preventing or detecting crime, that the surveillance is proportionate to the outcome sought, and that any risk of collateral intrusion has been identified and minimised.

The surveillance activity will not be **proportionate** if it is excessive in the circumstances of the case or if the information could be reasonably obtained by other less intrusive means.

Only the Chief Executive has the power to authorise directed surveillance involving the covert filming of any Elected Member, Corporate Director or Corporate Lead Officer.

Where several Agencies are working together, only one of them would need to obtain an authorisation for covert activity.

If during the course of the operation those activities change, there will be a need to apply for a review authorisation.

Role of the Investigating Officer – Applicant

The role of the Applicant is to present the facts of the application for covert surveillance including:

- The crime to be investigated;
- Reason why it is proposed to conduct the Investigation covertly;
- What covert tactics are requested;
- Why the covert tactics requested;
- Who the covert surveillance will be focused on;
- Who else will be affected by it;
- How it is intended to conduct the covert surveillance; and
- Provide facts and evidence.

The Applicant is not required to assert that the actions to be taken are necessary and proportionate- that is the statutory responsibility of the AO.

Completing the Forms

The Council Officer will need to make an application on the relevant form, which can be downloaded from the Home Office website, https://www.gov.uk/government/collections/ripa-forms--2

Application forms for directed surveillance will need to contain the following information:

- The action that needs to be authorised;
- If known, the identities of the people who are going to be the subject of the directed surveillance;
- An account of the investigation;

- An explanation of the techniques that you intend to use;
- Confirmation that the action proposed is intended to prevent crime or detect crime;
- An explanation of why the directed surveillance is considered to be proportionate to the outcome it seeks to achieve;
- An explanation of the information which is hoped to be obtained;
- An assessment of the potential for collateral intrusion (i.e., what interference will there be with the privacy of persons other than the subjects of the surveillance;
- Whether any confidential information will be acquired;
- If authorisation is needed urgently, the reasons for the urgency;
- Sequential Unique Reference Number (URN) obtained from the SRO and entered on to the form; and
- The form should specify the type of 'crime' involved – application forms should be explicit. General use of word 'crime' is not sufficient. Fishing expeditions are not appropriate.

Example forms (with guidance on filling in the forms) are available from the Council's Intranet Site (CeriNet) at [enter web link]). **Flowchart 3** will also assist.

Officers making an application and Authorising Officers should also be aware of, and have regard to:

- **Home Office Covert Surveillance and Property Interference Revised Code of Practice 2018;**
- **OSC Procedures & Guidance Document;**
- **This RIPA Policy; and**
- **ACT NOW Toolkit.**

Note: Standard wording should not be used when completing authorisations. The explanation and information provided on the authorisation should relate to the individual facts of the case and state clearly the objectives of the surveillance.

The Role of the Authorising Officer ('AO')

Once an authorisation has been granted, the Authorising Officer will consider the duration of the authorisation, renewal of the authorisation and cancellation of the authorisation.

Note: The notices and authorisations do not take effect until a Magistrate has approved the authorisation. See below for the procedure for seeking such approval.

Directed Surveillance authorisations cease to have effect 3 months from the date of approval.

RIPA and the associated Codes require that when the Council undertakes '*covert directed surveillance'*, uses a CHIS or access communications data, these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 N0.521) states that the AOs for a local authority can be a Director, Head of Service, Service Manager or equivalent.

Services may, therefore, currently nominate officers from at least Corporate Lead Officer level, who can authorise these activities either as an AO for the purposes of directed covert surveillance or use of a CHIS.

Pursuant to the Council's corporate restructure, effective from 1st April 2018, and further to Council resolution made on the 21st June 2018, the following officers are authorised to act as AOs:

- **Corporate Lead Officer: People and Organisation;**
- **Corporate Lead Officer: Policy, Performance & Public Protection; and**
- **Corporate Lead Officer: Porth Cynnal.**

Where the surveillance involves the likelihood of obtaining confidential information or the deployment of juveniles or vulnerable people (see below), then the authorisation **must** be sought from the Chief Executive or, in their absence, the acting Chief Executive.

If there is any doubt regarding sufficiency of rank, contact the SRO (Monitoring Officer/CLO – Legal and Governance) for advice.

Care must be taken where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality may be involved.

Where such material has been acquired and retained, the SRO must be informed as soon as possible, as the matter should be reported to the IPCO during their next inspection and the material should be made available to the IPCO, if requested.

In authorising any applications for directed surveillance, and in considering any renewals, reviews and cancellations, the Authorising Officer should also consider:

(a) how long will the data be retained for?; and

(b) is this compliant with the Council's Information and Records Management Policy and Corporate Retention Schedule?

(see Part 4 below).

Renewals

The Authorising Officer can renew an authorisation before it expires if it is necessary for the authorisation to continue for the purpose it was originally given.

An application for renewal must not be made more than 7 working days before the authorisation is due to expire. This is to ensure that the renewal is necessary.

Authorisations may be renewed more than once provided they continue to meet the criteria.

Applications for renewals must be made on another form which can be downloaded from the Home Office website (example forms (with guidance on how to fill in the forms) are available on the Council's Intranet Site (CeriNet) at [enter web link]), and see Paragraphs 5.16-21 of the Home Office Code of Practice for Directed Surveillance and Property Interference Revised Code of Practice 2018).

Note: Renewals do not take effect until a Magistrate has approved the authorisation.

Reviews

When the authorisation is granted, the AO will determine how often reviews should take place. Reviews will consider whether the authorisation is still needed i.e. whether the surveillance should continue.

Reviews do not require judicial approval and can be conducted internally (see Paragraphs 9.11-13 of the Home Office Code of Practice for Directed Surveillance and Property Interference).

The AO should consider the use of the tactics to date, along with their impact and any product, to ensure that each additional tactic is necessary, whether collateral intrusion can be justified, and whether the cumulative effect of the tactics is proportionate in light of progress.

Any amendments must be explicit, and no tactic may be used prior to it being granted by the AO.

The AO should clearly set out what activity and surveillance equipment is authorised in order that those conducting the surveillance are clear on what has been sanctioned at each stage in the authorisation process.

An audit trail of the review criteria should be kept.

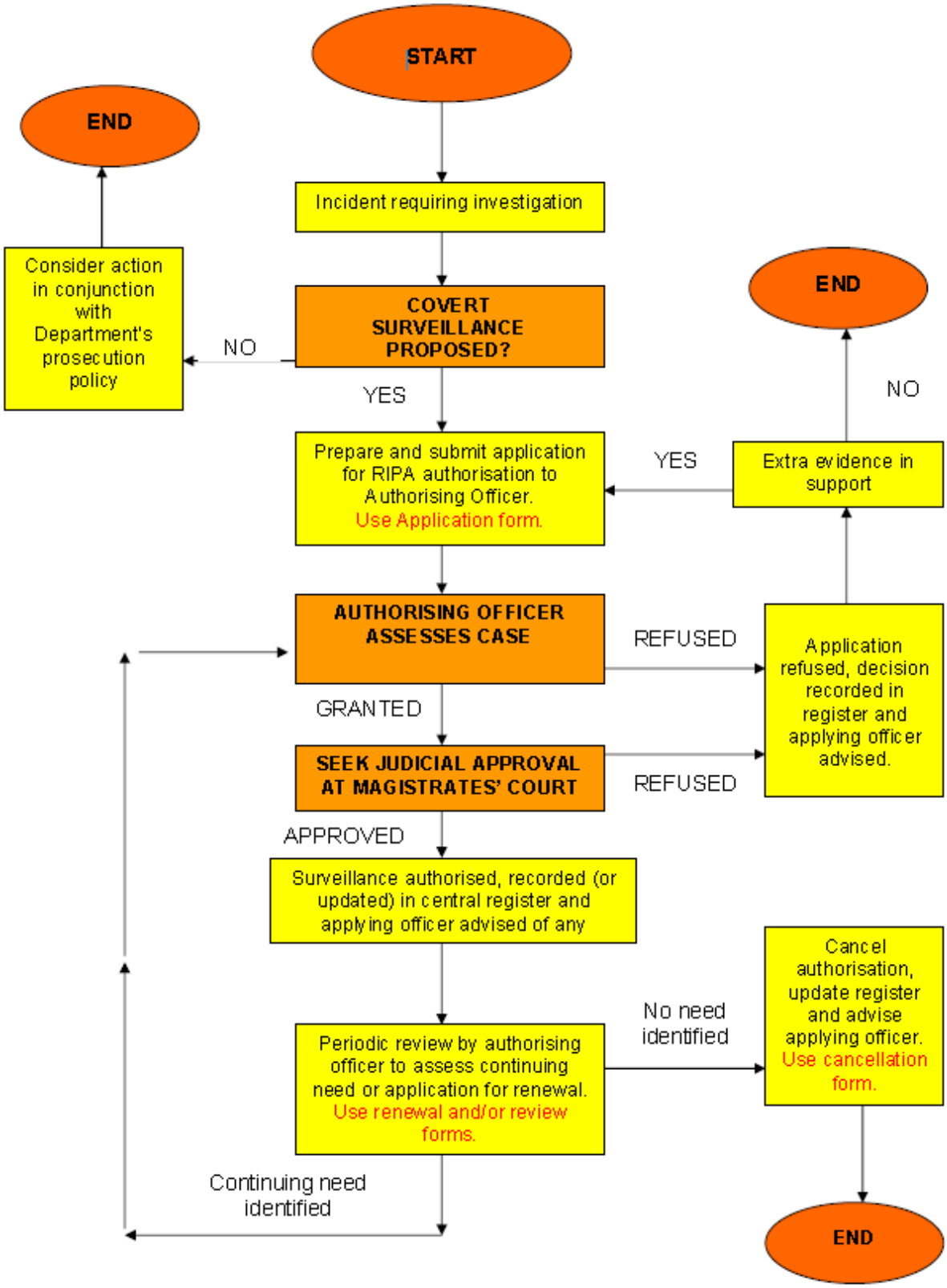
Cancellations

Authorisations will be cancelled when the AO is satisfied the criteria for authorisation is no longer met. To cancel the authorisation, the officer in charge of the investigation should complete a cancellation form (found on the Home Office website and Appendices to this document). This form should then be checked by the officer's manager, and it should then be sent to the AO. The cancellation form must contain the date of cancellation. The form will also require an explanation of reasons for cancellation, the value of the surveillance, and AO's statement (to include directions for management and storage of the product of surveillance).

See Paragraphs 5.22-27 of the Directed Surveillance and Property Interference Revised Code of Practice 2018.

Cancellations do not require judicial approval.

Flowchart 3 – Basic Lifecycle of a Directed Surveillance Authorisation (Similar lifecycle for a CHIS)



Guidance for Authorising Officers on Authorising Directed Surveillance Applications

Section 27 of RIPA provides a defence if covert surveillance is challenged:

'(1) Conduct to which this Part applies shall be lawful for all purposes if -
(a) an authorisation under this Part confers an entitlement to engage in that conduct on the person whose conduct it is; and
(b) His conduct is in accordance with the authorisation.'

To take advantage of this defence, the surveillance needs to be properly authorised. S.28 sets out the criteria for authorising Directed Surveillance, whilst S.29 covers CHIS.

Time Limits

The current time limit for a Directed Surveillance authorisation is 3 months.

A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by a Magistrate.

An application for renewal must not be made more than 7 working days before the authorisation is due to expire. This is to ensure that the renewal is necessary but local authorities must take account of factors, which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a Magistrate to consider the application).

Authorising Officer's Considerations

S.28 (2) of RIPA states:

> *'A person shall not grant an authorisation for the carrying out of directed surveillance unless he believes –*
>
> *(a) that the authorisation is necessary on grounds falling within subsection (3); and*
> *(b) that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.'*

*See **Flowchart 4** to assess whether Directed Surveillance should be authorised.*

It is the role of the AO to consider the following factors.

A. Is the surveillance necessary?

The surveillance has to be necessary on one of the grounds set out in S.28 (3). Previously local authorities could authorise Directed Surveillance where it was necessary

> *'for the purpose of preventing or detecting crime or of preventing disorder.' S.28(3)(b))*

The Home Office Review, which reported in January 2011, recommended that where local authorities wish to use Directed Surveillance, this should be confined to cases where the offence under investigation is a serious offence.

This recommendation was put into effect by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 which was made in June 2012 and came into force on 1st November 2012. This amends the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521 ('the 2010 Order'), which prescribes which officers, within a public authority, have the power to grant authorisations for the carrying out of Directed Surveillance and the grounds, under Section 28(3), upon which authorisations can be granted.

The Council's AOs may **not** authorise Directed Surveillance unless it is for the purpose of preventing or detecting conduct which constitutes a criminal offence, or is a criminal offence, and it meets the conditions set out in the new Article 7A(3)(a) or (b) of the 2010 Order. Those conditions are that:

a) The criminal offence which is sought to be prevented or detected is **punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment**, or

b) Would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. The latter are all offences involving sale of tobacco and alcohol to underage children.

Surveillance being carried out to tackle disorder (e.g. anti-social behaviour) can no longer be authorised as Directed Surveillance, unless the disorder includes criminal offences satisfying the above criteria.

No RIPA authorisation is necessary for:

- Immediate response;
- General observation activities;
- Overt CCTV/APNR systems;
- TV detector vans;
- Overt recording of noise nuisance;
- Interview with members of the public;
- Covert recordings for noise nuisance, when the recording is in decibels or constitutes non-verbal noise, or is of verbal content made at a level which does not exceed that which can be heard with the naked ear (see Covert Surveillance and Property Interference Revised Code of Practice 2018 at para 3.40); nor
- Overt and covert recording of voluntary interviews with members of the public.

The AO should clearly set out what activity and surveillance equipment is authorised in order that those conducting the surveillance are clear as to what has been sanctioned at each stage in the authorisation process. It is recognised that it is not always possible, at the outset of an investigation, to foresee how it will progress. However, this should not be a reason for Applicants to request a wide number of tactics/techniques 'just in case' they are later needed.

The AO may not authorise more than that which can be justified at the time of the authorising decision, and should demonstrate control, and a proper understanding of necessity, collateral intrusion and proportionality, relating to each tactic/technique requested. AOs must ensure that legal requirements are addressed throughout the life of an authorisation.

B. Is the surveillance proportionate to what is sought to be achieved by carrying it out?

Proportionality means ensuring that the surveillance is the least intrusive method to obtain the required information having considered all reasonable alternatives. This requires consideration of not only whether surveillance is appropriate but also the method to be adopted, the duration and the equipment to be used.

It is necessary to balance the infringement against the benefit. The merit of each case is to be considered.

It is unacceptable to consider whether an authorisation is required based on the description of the surveillance alone. The legal principles must be applied to the particular facts, and is a matter of judgment.

The conduct that it is aimed to prevent/detect must be identified and clearly described, and an explanation provided of why it is necessary to use the covert techniques requested.

The AO may not authorise more that can be justified at the time of their decision and should demonstrate control, and a proper understanding of necessity, collateral intrusion and proportionality, relating to each tactic requested.

The OSC often states in its inspection reports that officers have not properly understood the concept of proportionality or have not demonstrated compliance within the authorisation form. The Covert Surveillance and Property Interference Revised Code of Practice 2018 (Para 4.7) requires four aspects to be addressed in the authorisation form:

1. Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
2. Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
3. Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
4. Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

The AO should consider the use made of tactics to date, along with their impact and any product to ensure that each additional tactic is necessary, whether collateral intrusion can be justified, and whether the cumulative effect of the tactics in proportionate.

The AO should set out in their own words why they believe the (RIPA) activity is necessary and proportionate. A bare assertion is not sufficient.

C. <u>Can Collateral Intrusion be avoided or minimised?</u>

The AO will need to carefully consider the likelihood of collateral intrusion occurring. This is the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation. If the risk is significant, measures should be taken, wherever practicable, to avoid or minimise any unnecessary intrusion.

Investigating Officers and AOs will need to ask themselves:

i. What is the impact on third parties? Is it significant? Can it be justified?
ii. If it is, what can be done to avoid or minimise it?
iii. Have the following been considered:
    - Changing the timing of the surveillance;
    - Reducing the amount of surveillance;

- Changing the method of surveillance;
- The nature of the private information likely to be obtained;
- The sensitivities of the local community; and
- Surveillance operations by other public authorities?

The need to obtain the best evidence to investigate the crime will be paramount at all times.

Next Stage: Once the surveillance has been authorised the next stage is to seek Magistrate's approval (see below).

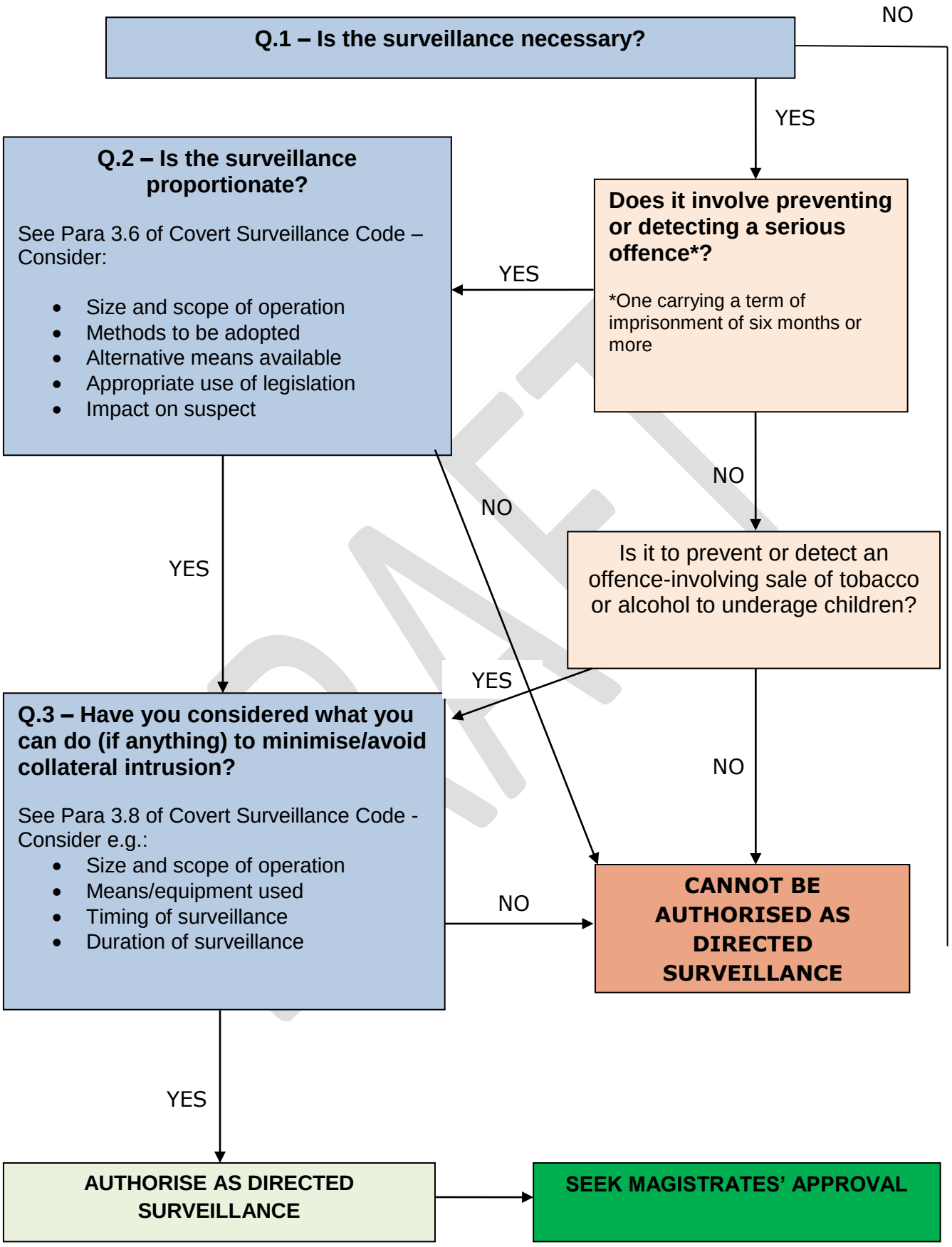
AOs must also, through their relevant Data Controller, ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and any relevant internal arrangements produced by the Council relating to the handling and storage of material (see Paragraphs 9.1.4 to 9.2.2 of The Covert Surveillance and Property Interference Revised Code of Practice 2018 and Assurance of Data Handling and Retention Safeguards section below). Within the Council, this is the Data Protection Officer, who will report to the Council's Senior Information Risk Owner ('SIRO').

As set out above (and Part 4 below), in authorising any applications for directed surveillance, the Authorising Officer should also consider:

(a) how long will the data be retained for?; and

(b) is this compliant with the Council's Information and Records Management Policy and Corporate Retention Schedule?

Flowchart 4 - Authorising Directed Surveillance



SEEKING MAGISTRATE'S APPROVAL (JUDICIAL APPROVAL) FOR DIRECTED SURVEILLANCE

Background

Chapter 2 of Part 2 of the Protection of Freedoms Act 2012 (sections 37 and 38) came into force on 1st November 2012. This changed the procedure for the authorisation of Council surveillance under RIPA and approval of a Magistrate is needed for the use of Directed Surveillance.

An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. There is no requirement for the Magistrate to consider either cancellations or internal reviews.

Home Office Guidance

The Home Office has published guidance on the Magistrate's approval process for both local authorities and the Magistrate's Court:
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

This guidance is non-statutory but provides advice on how local authorities can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the two statutory Codes of Practice made under RIPA.

See Flowchart 5 for summary of the Magistrates approval process

The Magistrate's Approval Process

1. The first stage will be to apply for an internal authorisation in the usual way. Once this has been granted, the local authority will need to contact the local Magistrates' Court to arrange a hearing.

2. The hearing constitutes legal proceedings. Therefore, local authority officers need to be formally designated to appear before the magistrate, take the oath, present evidence or provide information, as required, to support the application. The Council will need to formally designate officers for this purpose under section 223 of the Local Government Act 1972, to represent the Council within the proceedings.

3. The Home Office suggests that the Investigating Officer will be best suited to fulfil this role but the AO may also want to attend to answer any questions.

4. The local authority will provide the Magistrate with a copy of the original RIPA authorisation. This forms the basis of the application to the Magistrate and should contain all information that is relied upon. In addition, the local authority will provide the Magistrate with two copies of a partially completed judicial application/order form, which is included in the Home Office Guidance (example forms (with guidance on filling in the forms) are available from the Council's Intranet Site (CeriNet) at [enter web link])).

5. The hearing will be held in private and heard by a single Magistrate who will read and consider the RIPA authorisation and the judicial application/order form. She/he may

have questions to clarify points or require additional reassurance on particular matters. The forms and supporting papers must by themselves make the case. **It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.**

6. The Magistrate will consider whether they are satisfied that, at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition the Magistrate must be satisfied that the Authorising Officer was of appropriate designation within the local authority and that the authorisation was made in accordance with any applicable legal restrictions (e.g. meets the Serious Crime Test for Directed Surveillance)

7. The order section of the above mentioned form will be completed by the Magistrate and will be the official record of his/her decision. The Council will need to retain a copy of the form after it has been signed by the Magistrate.

Magistrate's Options

The Magistrate may decide to –

- ***Approve the grant/renewal of the authorisation***

The grant/renewal of the authorisation will then take effect and the Council may proceed to use the surveillance technique mentioned therein.

- ***Refuse to approve the grant/renewal of the authorisation on a technicality***

The RIPA authorisation will not take effect and the Council may not use the surveillance technique in that case. The Council will need to consider the reasons for the refusal. A technical error in the form may be remedied without the need to go through the internal authorisation process again. The Council can then reapply for Magistrate's approval.

- ***Refuse to approve the grant/renewal and quash the authorisation***

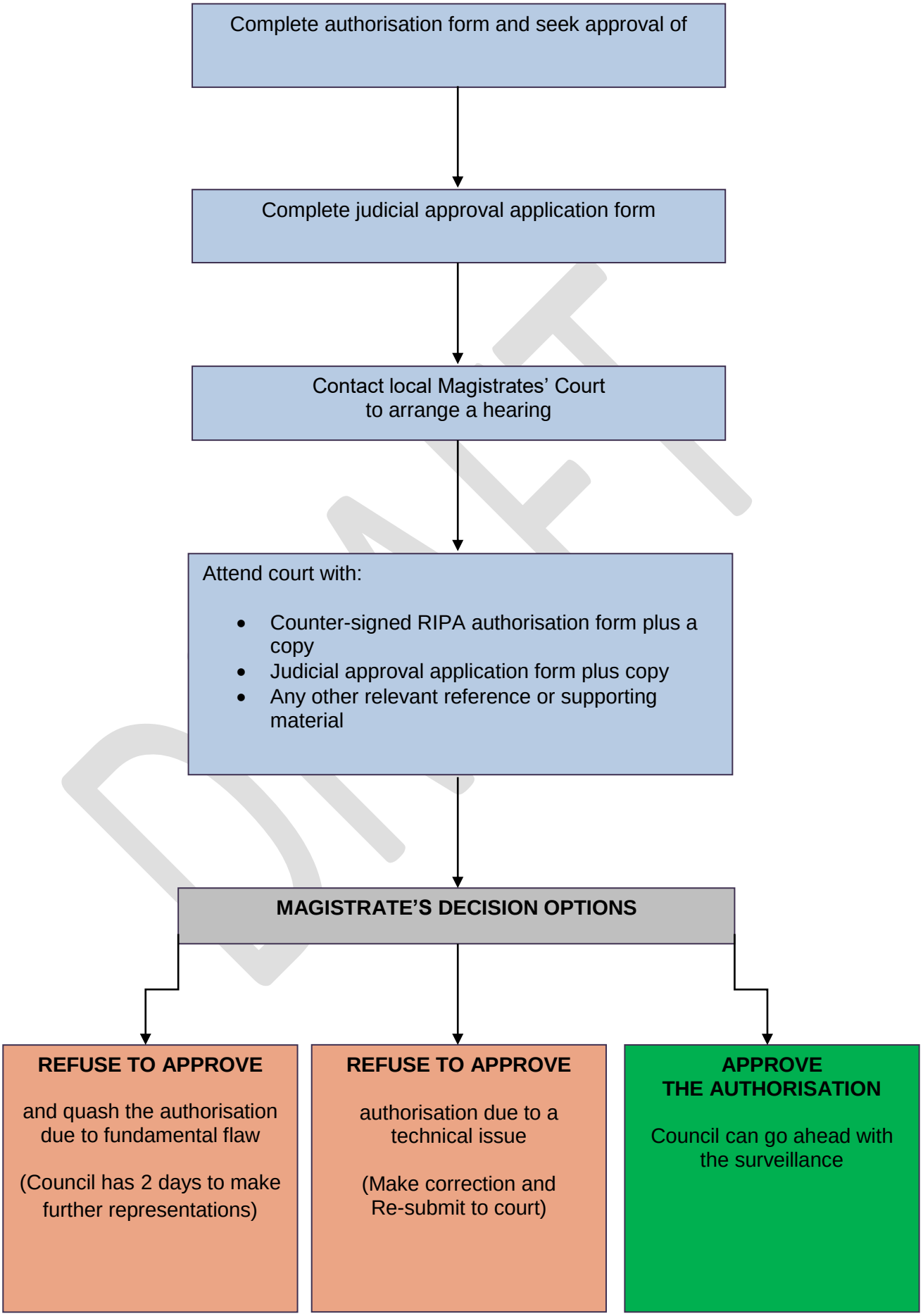
A Magistrate may refuse to approve the grant or renewal of an authorisation and decide to quash the original authorisation. This may be because they believe it is not necessary or proportionate. The RIPA authorisation will not take effect and the Council may not use the surveillance technique in that case. The Magistrate must not exercise their power to quash the authorisation unless the local authority has had at least two business days from the date of the refusal in which to prepare and make further representations to the court.

Appeals

There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee. Therefore, the Council may only appeal a Magistrate's decision to refuse approval of an authorisation, on a point of law by making an application for Judicial Review in the High Court.

The Investigatory Powers Tribunal ('IPT') will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT finds fault with a RIPA authorisation, it has the power to quash the Magistrate's order, which approved the grant or renewal of the authorisation. It can also award damages if it believes that an individual's human rights have been violated by the local authority (see Investigatory Powers Tribunal Rules 2018 (SI 2018/1334), which came into force on the 31st December 2018).

Flowchart 5- The Magistrate's Approval Process



PART 3 - Covert Human intelligence Source ('CHIS')

As stated above, Chapter 2 of RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities to ensure that they are compatible with the ECHR, particularly Article 8 (the right to respect for private and family life).

The first issue for any Council Officer who is considering undertaking covert surveillance is what type of surveillance they are undertaking, and **whether it is something that can be authorised under RIPA.** A CHIS is one of the two surveillance techniques available to the Council under Part 2 of Chapter 2 of RIPA. The second available technique is Directed Surveillance, but the third, Intrusive Surveillance, cannot be authorised by the Council.

Meaning of a 'CHIS'

A CHIS is defined in S.26(8) of RIPA:

'…a person is a covert human intelligence source if -

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

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

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

To ascertain whether a person is a CHIS three questions must be asked:

1. Is the person establishing or maintaining a personal or other relationship with a person?
2. Is that relationship being used for a covert purpose? and
3. Is the covert purpose facilitating the doing of anything falling within Paragraph (b) or (c) (above)?

See Flowchart 6 *to assess if the surveillance involves a CHIS.*

A CHIS is somebody who is concealing or misrepresenting their true identity or purpose in order to covertly gather or provide access to information from the target. Examples of a CHIS include a private investigator pretending to live on a housing estate to gather evidence of drug dealing or an informant who gives information to Trading Standards about illegal business practices in a factory or shop.

Under Age Sales

If the Young Person is briefed to enter into a conversation, which may lead to private 'information being obtained, then authorisation may be required'. If however, the Young Person is told not to communicate, and therefore no private information is obtained, then authorisation is not required.

Key Points to Note:

A. A public volunteer is not a CHIS. The Home Office Covert Human Intelligence Sources Revised Code of Practice 2018 (at Para 2.18) states:
'In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that is within their personal knowledge, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation under the 2000 Act is required.'

(*See Chapter 3 of the Code for further guidance on types of source activity to which authorisations under Part II RIPA may or may not apply)*

Care must be taken to ensure that someone who starts as a public volunteer does not end up being a CHIS.

B. There must be covert use of a relationship to provide access to information or to covertly disclose information. Merely giving a complainant a diary sheet to note comings and goings will not make that person a CHIS.

C. A test purchaser, in certain circumstances may require authorisation as a CHIS.

The Covert Surveillance and Property Interference Revised Code of Practice 2018 gives the following examples, to assist with the illustration and interpretation of certain provisions, but they are not provisions of the Code and are included only for guidance:

'**Example 3**: Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of public authorities and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.
Example 4*: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation.'*

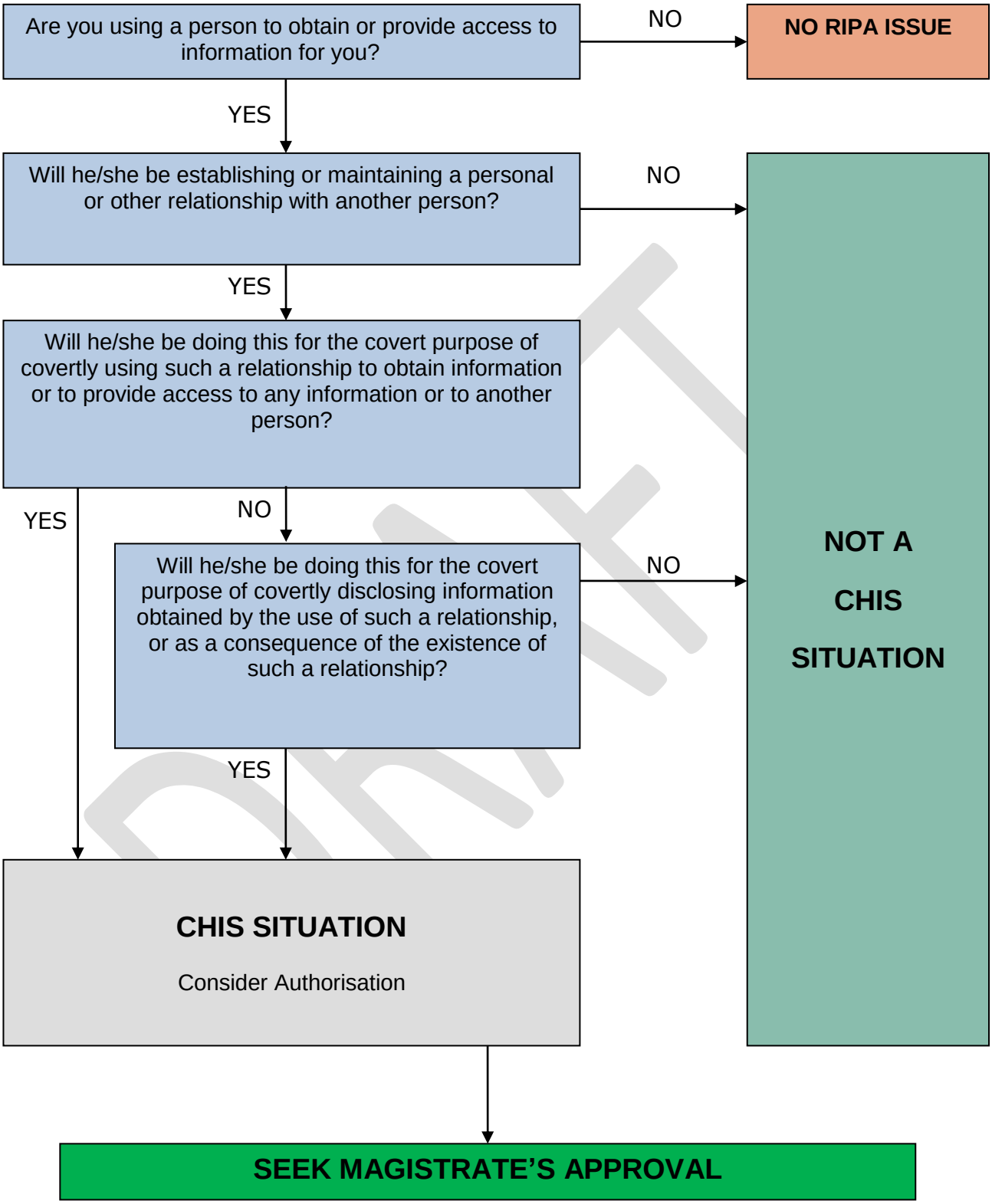
When considering underage test purchasing activities, investigating officers and Authorising Officer must also have regard to the:

- Age Restricted Products and Services: A Code of Practice for Regulatory Delivery (April 2014) (available at: https://www.gov.uk/government/publications/code-of-practice-age-restricted-products); and

- Pseudonyms/On-line personas
  Where these are permitted to be used corporately, the SRO will maintain a Register of these pseudonyms, together with details of which Services or officers who can use them/sanction their use.

  A regular check should then be made by Managers and/or the relevant Corporate Lead Officer of any such usage, including being able to review which media sites have been visited, when, for what purpose, and what has been done with any resultant product. Relevant Services are required to:
  - record information/date relating to covert social media/on-line surveillance;
  - identify a Designated Officer in the Service to collate the information;
  - provide this information to the Designated Officer; and
  - the Designated Officer is to provide the information to the SRO or SRO Representative every 4 months.

Flowchart 6 - Are you deploying a CHIS?



Procedure for obtaining authorisation for a CHIS under RIPA

Due to the statutory requirements that need to be adhered to when using a CHIS, it is unlikely that an investigation could involve the use of a CHIS without a lot of prior planning. Only in exceptional circumstances will Ceredigion County Council consider using CHIS as a surveillance method and assistance may be sought from the Police.

The Protection of Freedoms Act 2012 amended the 2000 Act to make CHIS authorisations by local authorities subject to judicial approval. These changes mean that local authorities need to obtain an order approving the grant or renewal of a CHIS authorisation from a Justice of the Peace before it can take effect.

If any Council Officer intends to use a CHIS, and requires advice and guidance, they should contact the SRO and/or the SRO's Representative **before any steps are taken**.

NB, as above, a public volunteer is not a CHIS.

Use of Juvenile CHIS

Special safeguards apply to the granting of authorisations where the CHIS would be a juvenile (under 18 years of age). Authorisations cannot be granted unless the provisions within The Regulation of Investigatory Powers (Juveniles) Order 2000 (https://www.legislation.gov.uk/uksi/2000/2793/contents/made) are satisfied. Home Office Guidance on using a Juvenile CHIS is also available: https://www.gov.uk/government/publications/covert-human-intelligence-sources-draft-code-of-practice/juvenile-accessible-version.

Where the surveillance involves the deployment of juveniles or vulnerable people as a CHIS, then the authorisation must be sought from the Chief Executive

If any Council Officer intends to use a Juvenile CHIS, and requires advice and guidance, they should contact the SRO and/or the SRO's Representative before any steps are taken.

Online Covert Activity – RIPA Social Media Policy

See the Council's RIPA Social Media Policy, which details Paragraph 4.11 of the Covert Human Intelligence Sources Revised Code of Practice 2018 (in relation to a CHIS authorisation), and which must be read in conjunction with this Policy.

Completing the Forms

An application must be made by the Officer on the relevant form, which can be downloaded from the Home Office website, https://www.gov.uk/government/collections/ripa-forms--2

Application forms will need to contain the following information:

- Details about the purpose for which the CHIS will be used;
- The identity, where known, to be used by the CHIS;
- Details of what the CHIS will be asked to do;
- Details of the investigation;
- Why the use of a CHIS is considered to be proportionate;
- Explanation of the information it is hoped will be obtained;
- The potential for collateral intrusion (i.e. interference with the privacy of people who are not subjects in the investigation);

- Likelihood of acquiring any confidential information; and
- Sequential Unique Reference Number (URN) obtained from the SRO and entered on to the form.

Officers making a CHIS application and Authorising Officers should also be aware of, and have regard to:

- The relevant Home Office Covert Human Intelligence Sources Code of Practice;
- This RIPA Policy; and the
- OSC Procedures and Guidance documents.

Example forms (with guidance on filling in the forms) are available from the Council's Intranet Site (CeriNet) at [enter web link]). **Flowchart 3** will also assist.

Note: As with directed surveillance application forms, standard wording should not be used when completing authorisations.

Before granting an authorisation, the Authorising Officer must be satisfied that the authorisation is necessary for the purpose of preventing and detecting crime. The Authorising Officer must also believe that using a CHIS is proportionate to the outcome sought and that there are adequate procedures in place for maintaining records of the operation. Collateral Intrusion will also need to be considered.

As set out in Part 4 below, in authorising any applications for a CHIS, the Authorising Officer should also consider:

(a) how long will the data be retained for?; and

(b) is this compliant with the Council's Information and Records Management Policy and Corporate Retention Schedule?

When using a CHIS, the Authorising Officer and the Officer who makes the application must have regard to section 29(5) of RIPA and also to The Regulation of Investigatory Powers (Source Records) Regulations 2000.

These provisions provide (amongst other things) the following:

- There will at all times be an officer within the Council who will have day to day responsibility for the CHIS;
- There will be another officer within the Council who will have general oversight over the use made of the CHIS;
- That records will document significant information connected with the security and welfare of the CHIS;
- That the tasks given to the CHIS and the uses made of the CHIS are recorded;
- The identity of the CHIS and the identity that is used by the CHIS; and
- That records are kept of all contacts and communications between the CHIS and the Council/ relevant officer at the Council.

The lifecycle of a CHIS authorisation

Once an authorisation has been granted, the Authorising Officer will consider the duration of the authorisation, renewal of the authorisation and cancellation of the authorisation.

Note: The notices and authorisations do not take effect until a Magistrate has approved the authorisation (this does not apply for communications data, which is dealt with by NAFN (see Part 4 below)).

CHIS authorisations cease to have effect 12 months from the date of approval. The duration of a juvenile CHIS authorisation is 1 month.

GUIDANCE FOR AUTHORISING OFFICERS AUTHORISING A CHIS: RULES AND CRITERIA

Section 27 of RIPA provides a defence if covert surveillance is challenged:

'1) Conduct to which this Part applies shall be lawful for all purposes if -

a. an authorisation under this Part confers an entitlement to engage in that conduct on the person whose conduct it is; and

b. his conduct is in accordance with the authorisation.'

To take advantage of this defence, the surveillance needs to be properly authorised.
S.29 sets out the criteria for authorising the use of a CHIS.

See **Flowchart 7** to assess whether to authorise a CHIS.

The Authorising Officer

RIPA and the associated Codes require that when the Council uses a CHIS, these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 N0.521) states that the AOs for a local authority can be a Director, Head of Service, Service Manager or equivalent.

Services may, therefore, currently nominate officers from at least Corporate Lead Officer level, who can authorise these activities either as an AO for the purposes of directed covert surveillance or use of a CHIS.

Pursuant to the Council's corporate restructure, effective from 1st April 2018, and further to Council resolution made on the 21st June 2018, the following Officers are authorised to act as AOs (the AOs are the same as those appointed to authorise Directed Surveillance applications):

- **Corporate Lead Officer: People and Organisation;**
- **Corporate Lead Officer: Policy, Performance & Public Protection; and**
- **Corporate Lead Officer: Porth Cynnal.**

As above, where the surveillance involves the likelihood of obtaining confidential information or the deployment of juveniles or vulnerable people, then the authorisation **must** be sought from the Chief Executive or, in their absence, the acting Chief Executive.

If there is any doubt regarding sufficiency of rank, contact the SRO or the SRO's Representative for advice.

As above, care must be taken where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality may be involved.

Where such material has been acquired and retained, the Council's Senior Responsible Officer for RIPA must be informed as soon as possible, as the matter should be reported to the IPCO during their next inspection and the material should be made available to the IPCO, if requested.

Authorising Officer's Consideration

S.29(2) states:

'A person shall not grant an authorisation for the conduct or the use of a covert human intelligence source unless he believes -

(a) that the authorisation is necessary on grounds falling within subsection (3);

(b) that the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use; and

(c) arrangements exist for the source's case that satisfy—

(i) the requirements of subsection (4A), in the case of a source of a relevant collaborative unit;

(iii) the requirements of subsection (5), in the case of any other source; and

that satisfy such other requirements as may be imposed by order made by the Secretary of State'

Please consult flowchart 7 when deciding whether the deployment of a CHIS should be authorised.

Three matters are important to consider before authorising the deployment of a CHIS:

1. Necessity

The deployment of a CHIS has to be necessary on one of the grounds set out in S.29 (3). Local authorities can only authorise on the one ground; where it is necessary:

'for the purpose of preventing or detecting crime or of preventing disorder.'
(S.29 (3) (b))

The matter being investigated must be an identifiable criminal offence or constitute disorder.

2. Proportionality

Proportionality means ensuring that the deployment of the CHIS is the least intrusive method to obtain the required information having considered all reasonable alternatives. This requires consideration of not only whether a CHIS is appropriate but also the method to be adopted, the duration and the equipment to be used. The CHIS Code (Para 3.5) requires four aspects to be addressed in the authorisation form:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and

- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

It is unacceptable to consider whether an authorisation is required based on the description of the surveillance alone. The legal principles must be applied to the particular facts, and is a matter of judgment.

The conduct that it is aimed to prevent/detect must be identified and clearly described, and an explanation provided of why it is necessary to use the covert techniques requested.

3. Security and Welfare Arrangements

CHIS's are often placed in difficult and sometime dangerous situations e.g. an informant on a housing estate in contact with criminal gangs. Appropriate security and welfare arrangements must also be in place in relation to each CHIS. S.29 (5) requires there to be:

- A person who will have day-to-day responsibility for dealing with the CHIS on behalf of that authority, and for his/her security and welfare;
- A person who will have general oversight of the use made of the CHIS. This person must be different to the one above;
- A person who will maintain a record of the use made of the CHIS. This can be any of the above or a separate person; and
- Proper and secure records to be kept about the use made of the CHIS.

Risk Assessment: An authorisation for the conduct or use of a CHIS may not be granted or renewed in any case where the source is under the age of eighteen at the time of the grant or renewal, unless a risk assessment has been carried out. This must be sufficient to demonstrate that:

- The nature and magnitude of any risk of physical injury to the CHIS arising in the course of, or as a result of, carrying out the conduct described in the authorisation has been identified and evaluated;

- The nature and magnitude of any risk of psychological distress to the CHIS arising in the course of, or as a result of, carrying out the conduct described in the authorisation has been identified and evaluated;

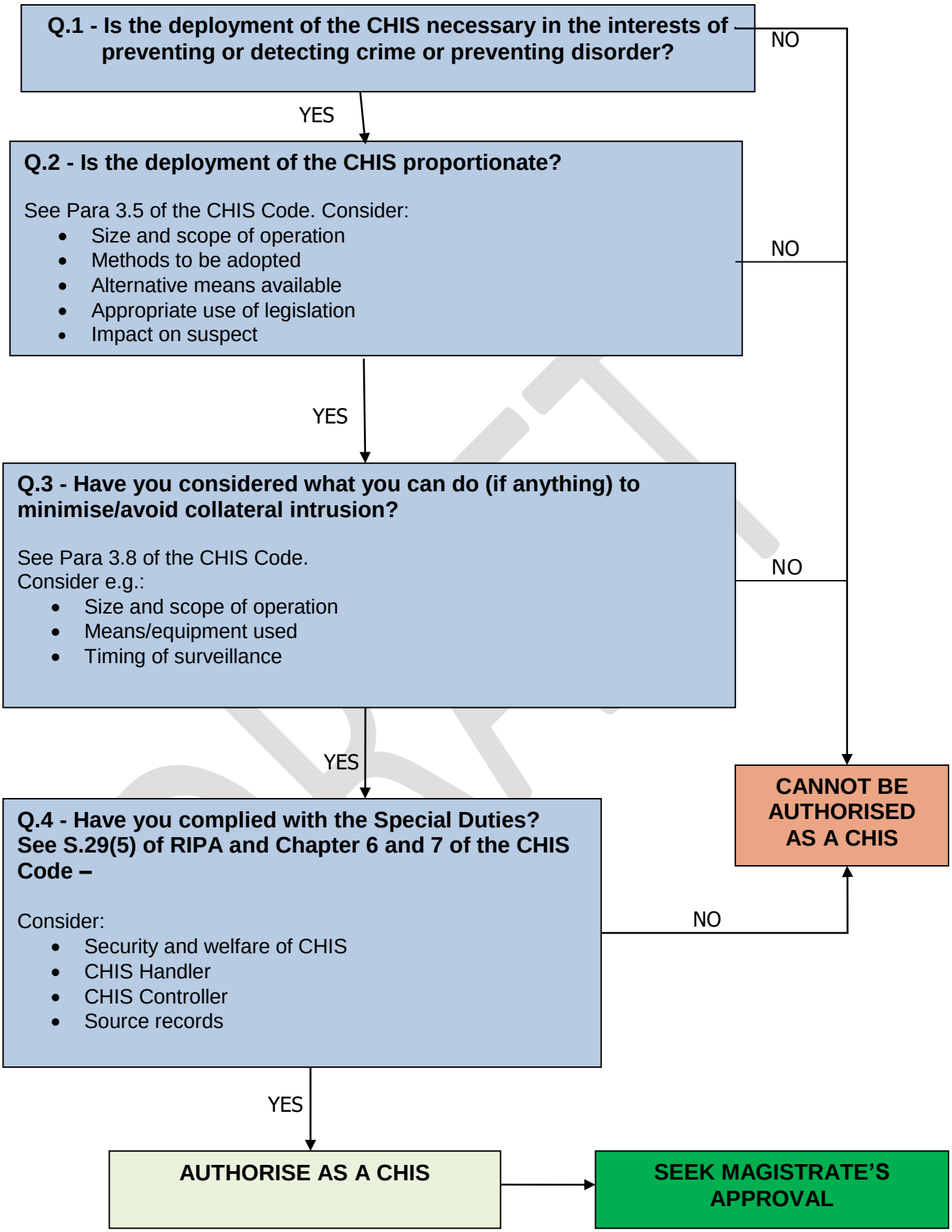
- The person granting or renewing the authorisation has considered the risk assessment and has satisfied himself that any risks identified in it are justified and, if they are, that they have been properly explained to and understood by the CHIS; and

- The person granting or renewing the authorisation knows whether the relationship to which the conduct or use would relate is between the CHIS and a relative, guardian or person who has for the time being assumed responsibility for the CHIS's welfare, and, if it is, has given particular consideration to whether the authorisation is justified in the light of that fact.

As stated above, in authorising any applications for a CHIS, the Authorising Officer should also consider:
(a) how long will the data be retained for?; and
(b) is this compliant with the Council's Information and Records Management Policy and Corporate Retention Schedule?

Next Stage: Once the use of a CHIS has been authorised, the next stage is to seek Magistrate's approval (see below).

Flowchart 7 – Authorising a CHIS



SEEKING MAGISTRATE'S APPROVAL FOR A CHIS (JUDICIAL APPROVAL)

Background

Since the 1st of November 2012 and the introduction of Chapter 2 of Part 2 of the Protection of Freedoms Act 2012 (ss37 and 38), local authorities are required to obtain the approval of a Magistrate for the deployment of a CHIS.

An approval is also required to renew an authorisation. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. There is no requirement for the Magistrate to consider either cancellations or internal reviews.

Home Office Guidance

The Home Office has published guidance on the Magistrate's approval process both for local authorities and the Magistrate's Court:
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/

This guidance is non-statutory but provides advice on how the Council can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the two statutory Codes of Practice made under RIPA.

The Magistrate's Approval Process (see also Flowchart 8 below)

1. The first stage will be to apply for an internal authorisation in the usual way. Once this has been granted, the Council will need to contact the local Magistrates' Court to arrange a hearing.

2. The hearing constitutes legal proceedings. Therefore, the Council's Officers need to be formally designated to appear before the Magistrate, take the oath, present evidence or provide information, as required, to support the application. The Council will need to formally designate Officers for this purpose under section 223 of the Local Government Act 1972, to represent the Council within the proceedings.

3. The Home Office suggests that the Investigating Officer will be best suited to fulfil this role, but the AO may also want to attend to answer any questions.

4. The Council will provide the Magistrate with a copy of the original RIPA authorisation. This forms the basis of the application to the Magistrate and should contain all information that is relied upon. In addition, the Council will provide the Magistrate with two copies of a partially completed judicial application/order form, which is included in the Home Office Guidance (example forms (with guidance on filling in the forms) are available from the Council's Intranet Site (CeriNet) at [enter web link])).

5. The hearing will be held in private and heard by a single Magistrate who will read and consider the RIPA authorisation and the judicial application/order form. The Magistrate may have questions to clarify points or require additional reassurance on particular matters. The forms and supporting papers must by themselves make the case. **It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided.**

6. The Magistrate will consider whether they are satisfied that, at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition the Magistrate must be satisfied that the Authorising Officer was of appropriate designation within the local authority and that the authorisation was made in accordance with any applicable legal restrictions (e.g. meets the Serious Crime Test for Directed Surveillance).

7. The order section of the above-mentioned form will be completed by the Magistrate and will be the official record of their decision. The Council will need to retain a copy of the form after it has been signed by the Magistrate.

Magistrate's Options

The Magistrate may decide to –

- ***Approve the grant/renewal of the authorisation***

The grant/renewal of the authorisation will then take effect and the Council may proceed to use the surveillance technique mentioned therein.

- ***Refuse to approve the grant/renewal of the authorisation on a technicality***

The RIPA authorisation will not take effect and the Council may not use the surveillance technique in that case. The Council will need to consider the reasons for the refusal. A technical error in the form may be remedied without the need to go through the internal authorisation process again. The Council can then reapply for Magistrate's approval.

- ***Refuse to approve the grant/renewal and quash the authorisation***

A Magistrate may refuse to approve the grant or renewal of an authorisation and decide to quash the original authorisation. This may be because they believe it is not necessary or proportionate. The RIPA authorisation will not take effect and the Council may not use the surveillance technique in that case. The Magistrate must not exercise their power to quash the authorisation unless the Council has had at least two business days from the date of the refusal in which to prepare and make further representations to the Court.

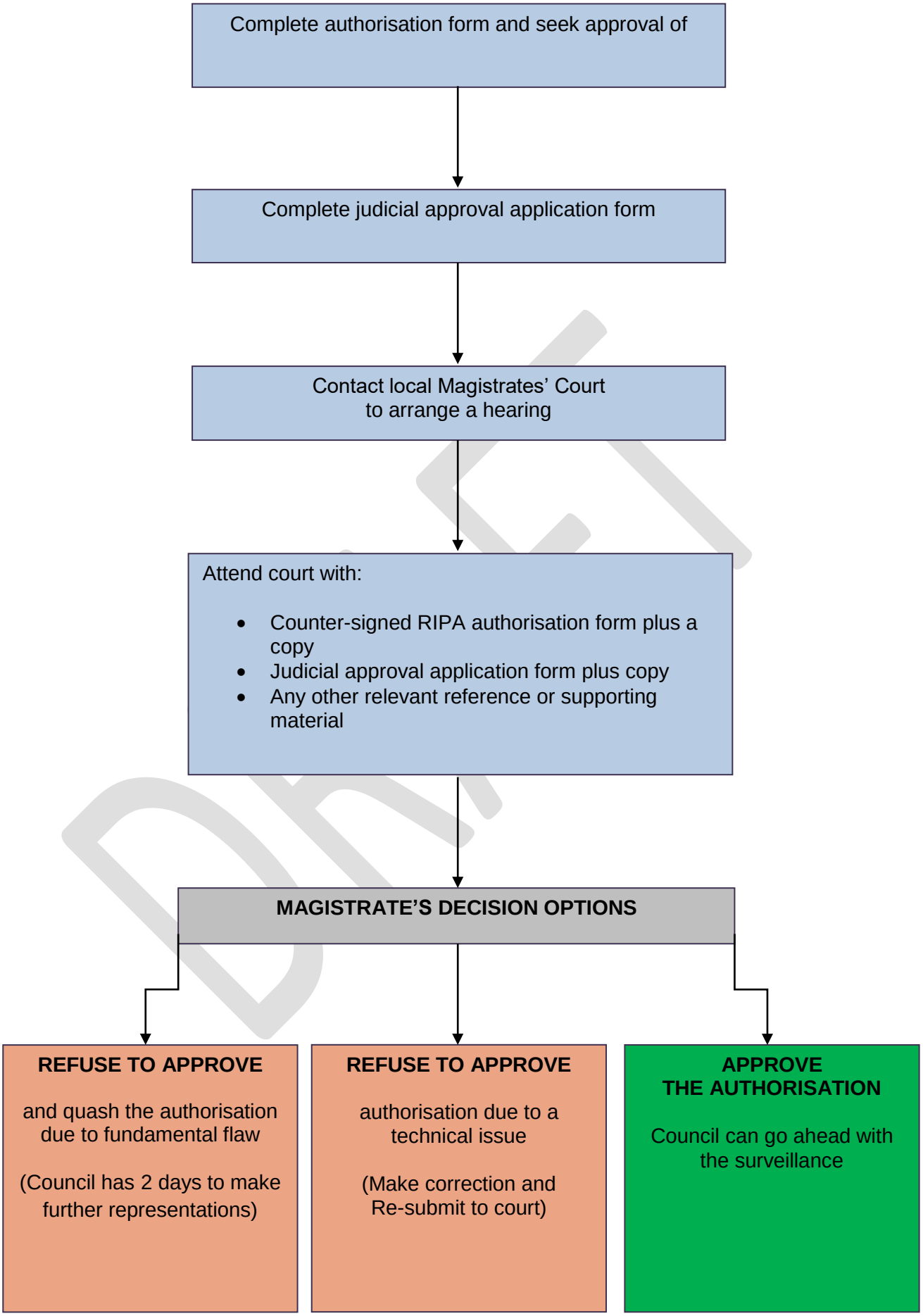
Appeals

There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee.

Therefore, the Council may only appeal a Magistrate's decision to refuse approval of an authorisation, on a point of law by making an application for Judicial Review in the High Court.

The Investigatory Powers Tribunal ('IPT') will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT finds fault with a RIPA authorisation, it has the power to quash the Magistrate's order, which approved the grant or renewal of the authorisation. It can also award damages if it believes that an individual's human rights have been violated by the Council (see Investigatory Powers Tribunal Rules 2018 (SI 2018/1334), which came into force on the 31st December 2018).

Flowchart 8 - The Magistrate's Approval Process (CHIS)



Time Limits

The current time limits for an authorisation to use a CHIS is 12 months for a CHIS or 1 month if the CHIS is underage.

A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by a Magistrate.

An application for renewal must not be made more than 7 working days before the authorisation is due to expire. This is to ensure that the renewal is necessary but local authorities must take account of factors, which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority authorising officer and a Magistrate to consider the application).

PART 4 RECORDS, DATA HANDLING, RETENTION SAFEGUARDS, ERRORS AND COMPLAINTS

THE CENTRAL REGISTER OF AUTHORISATIONS

A central register record of the following information relating to all authorisations will be held centrally by the SRO, with the Officer retaining a copy, and will be kept for at least 3 years from the ending of each authorisation, and in any event in compliance with the Council's Information and Records Management Policy (2019): https://cerinet.ceredigion.gov.uk/media/2725/information-and-records-management-policy-v20.pdf

Documentation of any instruction to cease surveillance must be retained. A record should be kept detailing the product obtained from the surveillance and whether objectives were achieved. Although the central register will be monitored by the SRO, it is ultimately the AO's responsibility to ensure renewals and cancellations are up to date.

Authorisations will be made available to the IPCO. It will be the responsibility of the SRO or nominated representative to ensure that the register is maintained and overseen.

The records should contain the following information:

- Original authorisation (not copies);
- The type of authorisation – e.g. Directed Surveillance or CHIS;
- The date the authorisation was given;
- The name and rank/grade of the authorising officer;
- The unique (sequential) reference number ('URN') of the investigation or operation;
- The title of the investigation or operation, including a brief description and names of subjects, if known;
- Whether the urgency provisions were used, and if so why;
- The date of any reviews;
- If the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- Whether the investigation or operation resulted in obtaining confidential information;
- Whether the authorisation was granted by an individual directly involved in the investigation;
- The date the authorisation was cancelled;
- Instruction to cease surveillance;
- Record of product obtained from the surveillance;
- Record of whether objectives achieved;
- Authorisations by Magistrates' Courts include date of Court hearing;
- Name of determining Magistrate, the time and date of the decision;
- Where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner;
- Record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner; and
- Where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

The Covert Surveillance and Property Interference Revised Code of Practice 2018 at Paragraph 8.2 also confirms that the following documentation should also be centrally retrievable for at least three years from the ending of each authorisation:

- A copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the AO;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the AO;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- The date and time when any instruction to cease surveillance was given;
- The date and time when any other instruction was given by the AO; and
- (For local authorities) A copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace ('JP').

All Investigating Officers should keep the authorisation within their own service and submit a copy to the SRO.

ASSURANCE OF DATA HANDLING AND RETENTION SAFEGUARDS

The procedures and safeguards to be applied in relation to the handling of any material obtained through Directed Surveillance under the 2000 Act is dealt with in detail in the Covert Surveillance and Property Interference Revised Code of Practice 2018 and Covert Human Intelligence Sources Code of Practice, which should be followed.

Application forms for RIPA Authorisations have been amended to include reference to retention periods, and confirmation that these periods are compliant with the Council's Information and Records Management Policy and Corporate Retention Schedule (example forms (with guidance on filling in the forms) are available from the Council's Intranet Site (CeriNet) at [enter web link])).

Authorisations must be kept for at least 3 years from the ending of each authorisation, and ideally up to five years. All data obtained under the IPA 2016 and RIPA must be clearly labelled and stored on a data pathway with a known retention policy.

The data pathway retention, review and disposal process must be in compliance with:

1. The Council's Information and Records Management Policy (2019): https://cerinet.ceredigion.gov.uk/media/2725/information-and-records-management-policy;

2. The Council's Corporate Retention Schedule (to follow);

3. The Covert Surveillance and Property Interference Revised Code of Practice 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf
   which states at Paragraph 8.5 - Retention of records:
   Records must be available for inspection by the Investigatory Powers Commissioner and retained to allow the Investigatory Powers Tribunal ('IPT'), established under Part IV of the 2000 Act, to carry out its functions. The IPT will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of the Act), particularly where continuing conduct is alleged. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to five years.

See also Paragraphs 8.6-8.7 below regarding errors.

4. Retention practices must comply with relevant legal frameworks including:
    - RIPA;
    - The IPA 2016;
    - The Data Protection Act 2018; and
    - Article 8(2) of the European Convention on Human Rights.

In authorising any applications relating to Directed Surveillance or a CHIS, AOs should also consider:
(a) how long will the data be retained for?; and
(b) is this compliant with the Council's Information and Records Management Policy and Corporate Retention Schedule?

AOs must also ensure that they fully understand any data pathways used for RIPA or IPA 2016 data.
Example: Directed surveillance data may be simultaneously stored on several data pathways, as follows:

- Pathway 1: CCTV video product is transferred onto a CD and kept in a secure cabinet;
- Pathway 2: a copy of the video is sent via email and stored on a common storage drive;
- Pathway 3: a copy of the video is received via email and saved in an Outlook folder by a legal officer; and
- Pathway 4: a copy of the video is received via email and stored in a password protected evidential casework folder by a legal officer.

Safeguarding processes must also comply with the Covert Surveillance and Property Interference Revised Code of Practice 2018 (available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf), which states at paragraph 9.3 that Public authorities '*should ensure that their actions when handling information obtained by means of covert surveillance or property interference comply with relevant legal frameworks and this code, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including data protection requirements, will ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards.*'

The Council must be compliant with data safeguards to establish a high level of confidence that all data obtained is retained lawfully, and to embed and encourage best practice for compliance, and also ensure that the handling of private information so obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards. Data must not be retained for longer than necessary or appropriate.

It is the responsibility of each service to securely retain all authorisations within their service and once an investigation is closed, the duplicate records held by the service should be disposed of in an appropriate manner i.e. treated as confidential waste and shredded.

AOs, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant internal arrangements produced by the Council relating to the handling and storage of material.

Any breaches of data protection requirements should also be reported to the Information Commissioner.

These safeguards will be subject to periodic review to ensure that they remain up-to-date and effective.

The Covert Surveillance and Property Interference Revised Code of Practice 2018 states:

- (*at Paragraph 9.5)* Safeguards (including privileged or confidential information): *Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of the code, something is necessary for the authorised purposes if the material:*

    - *is, or is likely to become, necessary for any of the statutory purposes set out in the 2000, 1997 or 1994 Act in relation to covert surveillance or property interference;*
    - *is necessary for facilitating the carrying out of the functions of public authorities under those Acts;*
    - *is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;*
    - *is necessary for the purposes of legal proceedings; or*
    - *is necessary for the performance of the functions of any person by or under any enactment.*

Paragraphs 9.14 to 9.22 of the Covert Surveillance and Property Interference Revised Code of Practice 2018 provide guidance as to the safeguards, which govern the dissemination, copying, storage and destruction of private information obtained through covert surveillance or property interference.

The Council must ensure that there are internal arrangements in force for securing that the requirements of the safeguards referred to in the Covert Surveillance and Property Interference Revised Code of Practice 2018 are satisfied in relation to private information obtained.

Training on Data Handling and Retention Safeguards can be arranged for any Authorising Officers or Officers who may handle such data – please contact the SRO if you would like to undertake any such Training.

Dissemination of information

The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose(s). This obligation applies equally to disclosure to additional persons within the Council, or another public authority, and to disclosure outside the Council, or other public authority. Similarly, only the material that is needed by the recipient must be disclosed e.g. if a summary of the material will suffice, no more than that summary should be disclosed.

This obligation to limit the number of persons to whom any of the information is disclosed, including the extent of the disclosure, to the minimum necessary for the authorised purpose(s) also applies to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the original authority before disclosing the material further. In others, explicit safeguards should be applied to any secondary recipients.

As confirmed in the Interception of Communications Data section above, regarding material obtained under a warrant or authorisation is disclosed to the authorities of a country or

territory outside the UK, the Council must ensure that the material is only handed over to the authorities if it appears to them that any requirements relating to minimising the extent to which material is disclosed, copied, distributed and retained will be observed to the extent that the authorising officer, Judicial Commissioner or Secretary of State considers appropriate.

Where material obtained under a warrant or authorisation is disclosed to the authorities of a country or territory outside the UK, the Council must ensure that the material is only handed over to the authorities if it appears to them that any requirements relating to minimising the extent to which material is disclosed, copied, distributed and retained will be observed to the extent that the authorising officer, Judicial Commissioner or Secretary of State considers appropriate.

Copying

Material obtained through covert surveillance or property interference may only be copied to the extent necessary for the authorised purposes. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance or property interference, and any record which refers to the covert surveillance or property interference and the identities of the persons to whom the material relates.

Storage

Material obtained through covert surveillance or property interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

The Council must apply the following protective security measures:

- Physical security to protect any premises where the information may be stored or accessed;
- IT security to minimise the risk of unauthorised access to IT systems; and
- An appropriate security clearance regime for staff, which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Deletion & Destruction

Information obtained through covert surveillance or property interference, and all copies, extracts and summaries, which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s). The duplicate records held by the service should be disposed of in an appropriate manner i.e. treated as confidential waste and shredded.

If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

Confidential and Legally Privileged Material

There are also very specific and detailed requirements in relation to particularly sensitive material, much of which is subject to enhanced authorisation regimes, this type of material includes:

- Material subject to legal privilege;
- Confidential personal information;
- Confidential constituent information; and
- Confidential journalistic material and journalists sources.

Surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material may be authorised only by AOs entitled to grant authorisations in respect of confidential or privileged information and care must be taken where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality may be involved.

Where such material has been acquired and retained, the Council's Senior Responsible Officer for RIPA must be informed as soon as possible, as the matter should be reported to the IPCO during their next inspection and the material should be made available to the IPCO, if requested.

Marking

Consideration should be given to appropriate marking of material, such as, for example, a marking of 'CONFIDENTIAL' or 'NOT TO BE DISTRIBUTED WITHOUT WRITTEN PERMISSION' on confidential or sensitive material.

Errors

Careful preparation and checking of authorisations and appropriate technical systems will reduce the scope for making errors.

The SRO will undertake an annual review of errors together with a written record.

See Paragraphs 8.6-8.18 Covert Surveillance & Property Interference Revised Code of Practice 2018:

> 8.6 This section provides information regarding errors. Proper application of the surveillance provisions provided for in Part II of the 2000 Act and the property interference provision provided for in the 1994 and 1997 Acts, should reduce the scope for making errors. Public authorities will be expected to have thorough procedures in place to comply with these provisions, including for example the careful preparation and checking of warrants and authorisations, reducing the scope for making errors.
>
> 8.7 Wherever possible, any technical systems should incorporate functionality to minimise errors.
>
> 8.8 An error must be reported if it is a 'relevant error'. Under section 231(9) of the Investigatory Powers Act 2016, a relevant error for the purpose of activity covered by this code is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act or the property interference provisions of the 1994 and 1997 Acts. Examples of relevant errors occurring would include circumstances where:
>
> - Surveillance or property interference activity has taken place without lawful authorization; or
> - There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Code.
>
> 8.9 Errors can have very significant consequences on an affected individual's rights and, in accordance with section 235(6) of the Investigatory Powers Act 2016, all

relevant errors made by public authorities must be reported to the Investigatory Powers Commissioner by the public authority that is aware of the error.

8.10 When a relevant error has occurred, the public authority that made the error must notify the Investigatory Powers Commissioner as soon as reasonably practicable, and no later than **ten working** days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the Investigatory Powers Commissioner. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

8.11 From the point at which the public authority identifies that a relevant error may have occurred, they must take steps to confirm the fact of an error as quickly as it is reasonably practicable to do so. Where it is subsequently confirmed that an error has occurred and that error is notified to the Commissioner, the public authority must also inform the Commissioner of when it was initially identified that an error may have taken place.

8.12 A full report must be sent to the Investigatory Powers Commissioner as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days (or as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report should include information on the cause of the error; the amount of surveillance or property interference conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

8.13 The Investigatory Powers Commissioner may issue guidance as necessary, including guidance on the format of error reports. Public authorities must have regard to any guidance on errors issued by the Investigatory Powers Commissioners.

8.14 In addition to the above, errors may arise where a warrant or authorisation has been obtained as a result of the public authority having been provided with information which later proved to be incorrect due to an error on the part of the person providing the information, but on which the public authority relied in good faith. Whilst these actions do not constitute a relevant error on the part of the authority which acted on the information, such occurrences should be brought to the attention of the Investigatory Powers Commissioner. Where reporting such circumstances to the Investigatory Powers Commissioner, the processes outlined at Paragraph 8.10 apply as they apply to the reporting of a relevant error.

Examples of common mistakes in RIPA Forms

- Using out of date Home Office forms;
- Not quoting URN;
- Copying wording from old authorisations;
- Failing to give detailed explanations of what the surveillance will involve;
- Failing to sufficiently consider and/or explain the proportionality factors;
- Failing to sufficiently consider and/or explain Collateral Intrusion;
- Failing to sufficiently consider likelihood of obtaining confidential information;
- Failing to send (original) completed forms to the SRO; or

- Failure to request only the tactics known to be available and intended to be used.

Examples of Authorising Officers' Mistakes

- Repetitive narrative and rubber stamping without proper consideration of all the facts set out in the authorisation form;
- Failure to clearly set out what activity and surveillance equipment is authorised;
- Not knowing the capability of the surveillance equipment which is being authorised; E.g. cameras that record continuously, thermal image/infrared capability, cameras activated by motion);
- Failing to demonstrate that less intrusive methods have been adequately considered and why they have been discounted in favour of the tactic selected;
- Failing when cancelling authorisations, to give directions for management and storage of the product of the surveillance;
- No robust and quality assurance procedures;
- Failure to evidence proportionality – that other means have been considered, and that the relevant criteria has been considered; or
- The need for authorisation has to be judged at the time of the authorisation, not with the benefit of hindsight.

Serious Errors

8.15 Section 231 of the 2016 Act states that the IPC must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

8.16 In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

- national security;
- the prevention or detection of serious crime;
- the economic well-being of the United Kingdom; or
- the continued discharge of the functions of any of the intelligence services.

8.17 Before making their decision, the Commissioner must ask the public authority which has made the error to make submissions on the matters concerned. Public authorities must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

8.18 When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

Further guidance can be found in:

- Para 7.1 – 7.20 of the Covert Human Intelligence Sources Revised Code of Practice 2018 and
- Para 8.6 – 8.18 of the Covert Surveillance and Property Interference Revised Code of Practice 2018.

COMPLAINTS

Any individual who is dissatisfied about the way the Council has or is carrying out surveillance may make a complaint. The decision as to which procedure should be used lies with the individual concerned.

If a person wishes to complain using the Council's procedures, then the complainant should be made aware of the Council's Corporate Complaints Procedure (see https://www.ceredigion.gov.uk/your-council/comments-compliments-and-complaints/corporate-complaints/
and https://www.ceredigion.gov.uk/media/1179/complaints-policy-bookletenglish.pdf)
The complaint will be dealt with in accordance with that procedure.

If a person wishes to complain directly to an independent body or had used the Council's internal procedures and is still dissatisfied, then he/she may complain to the Investigatory Powers Tribunal ('IPT').

The IPT has jurisdiction to investigate and determine complaints against public authority use of investigatory powers. To find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com.

Complaints can be made in writing to:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

* See Part 5 below for complaints regarding Communications Data

Part 5 - Communications Data

The RIPA (Communications Data) Order 2010 (SI 2010 no. 480) came into force on the 6th of April 2010 and confirms the powers contained within Chapter 2 of RIPA provided to Local Authorities by the equivalent 2003 Order.

Chapter 2, in brief, allows a Public Authority, such as the Council, to acquire information defined as 'communications data'. This includes subscriber data and service data but not 'traffic data' as defined by RIPA.

It is the Investigatory Powers Act 2016 ('IPA 2016') that regulates access to Communications data (https://www.legislation.gov.uk/ukpga/2016/25/). See also the Communications Data Code of Practice 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf.

Meaning of 'Communications Data'

Communications data is *'information held by communication service providers (e.g. telecom, internet and postal companies) relating to the communication made by their customers*'. This includes information relating to the use of a communications service but does not include the contents of the communication itself.

A simple example of a successful application for communications data could include, for example, applying for details confirming an email's date and time, but not its content.

The Communications Data Code of Practice 2018 states (at paragraph 2.18) that 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 (the content of a communication is defined in section 261(6) of the IPA 2016 as any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of that communication).

The Communications Data Code of Practice 2018 states, in relation to Communications Data, that:

2.19 '*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.*

2.20 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email 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.

2.21 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

2.22 Communications data in relation to telecommunications operators' services and systems includes data held or obtainable by a telecommunications operator or postal operator or which is available directly from a telecommunication system and comprises four elements.

Data about an entity to which a telecommunications service is provided and relates to the provision of the service

2.23 This data includes information about any person or entity to whom a service is provided, whether a subscriber or guest user and whether or not they have ever used that service. For example, this may include information about the person associated with an email address even if that email address has not been used since its creation.

2.24 An entity (see below for further details) can also include devices so this data would cover information about the devices owned by a customer as well as the services provided by the telecommunications operator to which the owner of the devices subscribes. This data may include names and addresses of subscribers.

2.25 Importantly this data is limited to data held or obtained by the telecommunications operator in relation to the provision of a telecommunications service – it does not include data which may be held about a customer by a telecommunications operator more generally which is not related to the provision of a telecommunications service.

2.26 For example, for a social networking provider data such as the status of the account, contact details for the customer and the date a person registered with the service would all be communications data as they relate to the use of the service. However, other data held by the provider about a customer which does not relate to the provision of the telecommunications service, including personal information such as political or religious interests included in profile information, is not within scope of the definition of communications data.

Data comprised in, included as part of, attached to or logically associated with a communication for the purposes of a telecommunication system that facilitates the transmission of that communication

2.27 This data includes any information that is necessary to get a communication from its source to its destination, such as the dialled telephone number or Internet Protocol (IP) address. It includes data which:

- *identifies the sender or recipient of a communication or their location;*
- *identifies or selects the apparatus used to transmit the communication;*
- *comprises signals which activate the apparatus used (or which is to be used) to transmit the communication; and*
- *identifies data as being part of a communication.*

2.28 This element of the communications data definition also includes data held, or capable of being obtained, by the telecommunications operator which is logically associated with a communication for the purposes of the telecommunication system by which the communication is being, or may be, transmitted. In practice this will often mean any data which is used to route or transmit a communication which the telecommunications operator holds or could obtain, for example from the network.

Communications Data Code of Practice

2.29 This might include, for example data about domain name system ('DNS') requests which allow communications to be routed across the network. It also

includes data that facilitates the transmission of future communications (regardless of whether those communications are, in fact, transmitted).

2.30 Only information falling within this section of the definition of communications data can be obtained directly from a telecommunication system by a public authority.

Data which relates to the use of a service or system

2.31 This element includes other information held by a telecommunications operator about the use of the service such as information that the provider holds for billing purposes.

Data which is about the architecture of a telecommunication system.

2.32 The definition of communications data additionally includes data held by a telecommunications operator about the architecture of the telecommunication system (sometimes referred to as 'reference data'). This may include the location of cell masts or Wi-Fi hotspots. This information itself does not contain any information relating to specific persons and its acquisition in its own right does not interfere with the privacy of any customers. However, this data is often necessary for the public authority to interpret the data received in relation to specific communications or users of a service.

2.33 Part 3 of the Act does not apply to any conduct by a public authority to obtain publicly or commercially available communications data. A communications data authorisation under Part 3 is not mandatory to obtain reference data, such as mobile phone mast locations, from a telecommunications operator as there is no intrusion into an individual's rights. However, some reference data, such as details of Wi-Fi hotspots, may be commercially sensitive and an authorisation can be sought by a public authority seeking to obtain this data from a telecommunications operator where the telecommunications operator requires it.

Entity and Events Data

2.34 All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories:

- *entity data – this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices);*
- *events data – events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.*

2.35 The authorisation levels required to access communications data reflect the fact that the set of events data as a whole contains the more intrusive communications data, including information on who has been in communication with whom, a person's location when their mobile device connects to the network and internet connection records. The rank of the designated senior officer that can authorise acquisition of data reflects the differing levels of intrusiveness of the data. For example, in certain circumstances, the police can authorise access to entity data at Inspector level but events data is authorised at Superintendent level.

Additionally entity data can be obtained in a wider range of crime types than events data.

2.36 There are some circumstances where a telecommunications operator will need to process events data in order to respond to a request for entity data. In such circumstances the level of authorisation required is for the type of data that is to be disclosed, rather than the type of data that is processed e.g. where a public authority wants to know the identity of a person using an IP address at a specific time and date this will be an application for entity data.

2.37 Where a public authority provides events data to a telecommunications operator as part of a request for entity data then the telecommunications operator may disclose that events data in the response to the entity data authorisation. Taking the example above, the telecommunications operator could include the time and date of the communication as part of the response without the need for it to be authorised as an event. This is because the public authority, by providing the events data to the telecommunications operator, has demonstrated they are already aware of the event and only intend to determine the entity involved in that event. By disclosing the events data the telecommunications operator would only be providing the public authority with information they already knew. Such disclosure is likely to occur where the telecommunications operator discloses the full record from their systems.

Entity data

2.38 Entity data covers information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or describe the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore entity data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be events data.

2.39 Examples of entity data include:

- *'subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";*
- *subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;*
- *information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;*
- *information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes (This includes PUK (Personal Unlocking Key) codes for mobile phones. These are initially set by the handset manufacturer and are required to be disclosed in circumstances where a locked handset has been lawfully seized as evidence in criminal investigations or proceedings); and*
- *information about selection of preferential numbers or discount calls.*

2.40 Entity data can change over time. So, for example if a person moves house the address held by a telecommunications operator will change. The fact of that is an attribute of the entity (the person) and not a communication event.

2.41 Some telecommunications operators may choose to retain user passwords as clear text for business purposes (In many cases a telecommunications operator will actually retain a password hash rather than the password itself. When a user enters the password to use a service it is encrypted and the hash generated is checked against the hash already held by a telecommunications operator meaning the operator never needs to retain the actual password). In this context passwords would constitute entity data. Any information, such as a password, giving access to the content of any stored communications or access to the use of a communications service may only be sought under Part 3 of the Act from a telecommunications operator in the following circumstances:

- *where such information is necessary in the interests of national security; or*
- *for preventing death, injury or damage to health.*
-

2.42 A communications data authorisation cannot authorise a public authority to use a password obtained through that or another communications data authorisation. If a public authority wishes to use a password obtained through a communications data authorisation to access the content of stored communications or any communications service it must, in accordance with section 6

2.43 of the Act, ensure that it has appropriate lawful authority.

Events

2.44 Events data covers information about time-bound events taking place across a telecommunication system at a time interval. Communications data is limited to communication events describing the transmission of information between two or more entities over a telecommunications service. This will include information which identifies, or appears to identify, any person, apparatus ('Apparatus' is defined in section 263 of the Act to include 'any equipment, machinery or device (whether physical or logical) and any wire or cable') or location to or from which a communication is transmitted. It does not include non-communication events such as a change in address or telephone number for a customer.

2.45 Examples of events data include, but are not limited to:

- *information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);*
- *information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);*
- *information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;*
- *routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);*
- *itemised telephone call records (numbers called) (Itemised bills can include an indication of the cost for receiving communications, for example calls*

and messages received by a mobile telephone that has been 'roaming' on another network);

- *itemised internet connection records;*
- *itemised timing and duration of service usage (calls and/or connections);*
- *information about amounts of data downloaded and/or uploaded;*
- *information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.*'

Interception of Communications Data

The recording of telephone calls between two parties when neither party is aware of the recording cannot be undertaken by a local authority.

There may be situations where either the caller or receiver consents to the recording of the telephone conversation and, in such circumstances a warrant is not required. This type of surveillance will require authorisation, either as directed covert surveillance, or, if it is a CHIS making or receiving the telephone conversation (usually an officer working '*undercover*'), as a CHIS authorisation.

Where as part of an already authorised directed covert surveillance or CHIS a telephone conversation is to be recorded by the officer or the CHIS then no special or additional authorisation is required.

The recording of telephone conversations for purposes not connected with investigatory powers does not fall within the RIPA legislative framework.

The IPA 2016 sets out general duties in relation to privacy in relation to:

- unlawful interception of communications data and
- unlawful obtaining of communications data.

The Act also abolishes and restricts various general powers to obtain communications data and restricts the circumstances in which equipment interference, and certain requests about the interception of communications, can take place. The Act sets out prohibitions against unlawful interception.

Note that under section 11 IPA 2016, it is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority. An offence is not committed if the person obtaining the data can show that they acted in the reasonable belief that they had lawful authority.

It is not an offence to obtain communications data where this data is publicly or commercially available by a Telecommunications Operator/Postal Operator. In such circumstances the operator's consent provides the lawful authority. However, public authorities should not require, or invite, any operator to disclose communications data by relying on this exemption.

The IPA 2016 does not allow local authorities to intercept communications data. Officers of the Council are only permitted to obtain Communications Data through NAFN's SPOC (see below).

Communications Data authorisations cease to have effect 1 month from the date of approval. An authorised renewal can extend the authorisation for up to an additional month.

Failure to secure proper approval and to comply with the Council's Policy could lead to evidence being excluded by Courts, complaints against the Council, or the commission of criminal offences. The Council is subject to audit and inspection by the Investigatory Powers Commissioner's Office and it is important that we demonstrate compliance with IPA 2016.

Obtaining Communications Data through NAFN's SPOC

It is imperative that the acquisition of Communications Data is properly authorised.

Acquisition of communications data under the IPA 2016 involves four roles:

(a) Applicant;

(b) Approved Rank Officer ('ARO')

(c) Single point of contact ('SPOC');

(d) Senior Responsible Officer in a Public Authority ('SRO')

Authorising requests for Communications Data is done through the Council's membership of National Antifraud Network ('NAFN'), who act as an accredited SPOC with Telecoms Operators, Postal Operators and Internet Service Providers.

Officers authorised to seek the acquisition of any form of Communications Data (the Applicant) must apply for acquisition via NAFN's central SPOC portal. An Approved Rank Officer must also be aware of the application and NAFN facilitates the approval of the request by the Office for Communications Data Authorisations ('OCDA').

Since the IPA 2016 came into force, it has become the main legislation governing how public authorities including law enforcement agencies, intelligence agencies and local authorities use the investigatory powers available. These powers provide for the lawful acquisition of communications data including the details of who, where, when, how and with whom regarding a communication but not the contents (i.e. what is said).

To use the NAFN secured website, applicants have to individually register on the NAFN website at www.nafn.gov.uk. Once registered, the applicant completes the online application form and it is then submitted electronically to one of the SPOCs at NAFN, who will advise the AO of any need for changes. The relevant forms can also be downloaded from the Home Office website, and a copy can be obtained from the SRO or SRO Representative.

The application to acquire communications data must (per paragraphs 5.4-5.5 of the Communications Data Code of Practice 2018):

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;

- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

- include the operation name (if applicable) to which the application relates;

- identify and explain the time scale within which the data is required;

- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it (see Communications Data Code of Practice 2018 section on necessity and proportionality, beginning at paragraph 3.3. This also applies to the next two bullets on collateral intrusion and unintended consequences);

- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;

- consider and, where appropriate, describe any possible unintended consequences of the application; and

- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

- 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.

The NAFN officer appointed as SPOC, amongst other things, carries out a quality control role and advises on various matters to assist the investigating officer and the Approved Rank Officer in the Council for Communications Data Authorisations, who are required to be the same level of seniority (see 4.11 of the Communications Data Code of Practice 2018) to the Senior Responsible Officer for Communications Data.

The NAFN SPOC advises on whether the application meets the statutory requirements, whether the information being sought can be easily obtained by the Telecoms Operators, Postal operators or Internet Service Providers and whether the application would be cost effective. NAFN's SPOC will also be the contact officer for all liaisons with the Telecoms Operators, Postal Operators or Internet Service Providers.

The following officers currently undertake the role of '**Approved Rank Officers'** to confirm to NAFN that they are aware of the application made on behalf of the Council:

1. Corporate Lead Officer: Policy, Performance & Public Protection;

Alternative substitutes (if Approved Rank Officer 1 above unavailable);

- Corporate Lead Officer: People and Organisation; and
- Corporate Lead Officer: Porth Cynnal.

The Approved Rank Officer will receive notification, when the applicant completes the application, of the submission. Once they have confirmed they are aware of the application, the NAFN SPOC will receive the application and carry out appropriate checks on the application. If any fundamental changes are made to the application, the Approved Rank Officer will be required to confirm their awareness of the amended application. The Approved Rank Officer shall send a copy of the email to the SRO for Communications Data (see below).

Authorising Agency: Office for Communications Data Authorisations ('OCDA')

The IPA 2016 introduced the OCDA, the independent body responsible for the authorisation and assessment of all Data Communications applications under the IPA 2016. The OCDA carries out the following functions:

- Independent assessment of all Data Communications applications.
- Authorisation of any appropriate applications.
- Ensuring accountability of Authorities in the process and safeguarding standards.

Consequently, the acquisition of communications data by local authority Officers no longer requiring judicial approval. The application will be submitted by NAFN to the OCDA who will then assess the application. The NAFN SPOC then uses the authorisation process to obtain the required communications data from the Telecoms Operators/Postal Operators database and that data is posted on the website so that it can only be accessed by the applicant. If NAFN do not have direct access to the database of the relevant Telecoms Operators/Postal Operators their SPOC will send a notice to the Telecoms Operators/Postal Operators in the usual way.

Where the OCDA **authorises** the request, this decision is communicated to NAFN's SPOC (NAFN) and actions are taken to request the data from the relevant telecommunications providers and other agencies holding such communications data to provide the necessary data.

Where the OCDA requires the application to be **revised**, it will be returned via NAFN's SPOC and the Applicant will have 14 calendar days to revise the application and resubmit. Failure to revise the application within the 14 days will result in the application being automatically rejected.

Where the OCDA rejects the application, the Applicant can:

1. Cease to proceed with the application;
2. Re-submit the application with revised justification and/or a revised course of conduct to request the data; or
3. Re-submit the un-amended application and request a review of the decision by the OCDA.

In the case of seeking a review, or affectively appealing against the original determination **the Authority has 7 calendar days to seek the review**. Any appeal must be made by the Council's SRO. The OCDA will provide guidance on this process.

Using the NAFN portal has significant advantages and there is no other means of obtaining communications data, since the Code of Practice requires the Council to use the NAFN SPOC Service.

Both historical and future information may be sought from a provider, subject to limitations.

The Council's Senior Responsible Officer ('SRO') for Communications Data

The Council's **SRO for Communications Data** is the Monitoring Officer/Corporate Lead Officer – Legal & Governance

Any questions regarding Communications Data can be addressed to the SRO for Communications Data, or alternatively care of the **SRO Representative for Communications Data**, who is the Governance Officer.

The Communications Data Code of Practice 2018 (available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf) confirms at paragraph 4.10 that the Council should have a SRO for Communications Data. The SRO for Communications Data must be of a senior rank, which is at least the same rank as the designated senior officer (for NAFN's purposes, this would be a Council Director, Head of Service, Service Manager or a rank equivalent). Paragraph 4.10 of the Communications Data Code of Practice 2018 also states that the SRO for Communications Data is responsible for:

(a) the integrity of the process in place within the public authority to acquire communications data;

(b) engagement with Authorising Officers in the Office for Communications Data Authorisations (where relevant);

(c) compliance with Part 3 of the IPA 2016 and with the Communications Data Code of Practice 2018 , including responsibility for novel or contentious cases (see paragraph 8.45 of the Communications Data Code of Practice 2018);

(d) oversight of the reporting of errors to the Investigatory Powers Commissioner ('IPC') and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

(e) ensuring the overall quality of applications submitted to Office for Communications Data Authorisations ('OCDA') by the public authority;

(f) engagement with the IPC's inspectors when they conduct their inspections; and

(g) where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

Records kept must be held centrally by the NAFN SPOC and be available for inspection by the Investigatory Powers Commissioner's Office upon request and retained to allow the Investigatory Powers Tribunal ('IPT'), to carry out its functions. The retention of documents service will be provided by NAFN, who shall also provide copies periodically, and as requested, to the SRO for Communications Data (see also paragraphs 24.1 – 24.9 of the Communications Data Code of Practice 2018).

For further information regarding Communications Data acquisition and disclosure, retention and general matters see the Communications Data Code of Practice 2018: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf.

Communications Data Errors

Where any error occurs, in the giving of a notice or authorisation or as a consequence of any authorised conduct or any conduct undertaken to comply with a notice, a record should

be kept. An error can only occur after the notice has been served on the Telecoms Operators/Postal Operators, so if it is discovered before this point it does not officially count as an error.
See paragraphs 24.17 – 24.37 of the Communications Data Code of Practice 2018.

There are 2 types of errors namely '**Reportable Errors'** and '**Recordable Errors'**:

- **Reportable Errors** are ones where communications data is acquired wrongly and in this case a report must be made to the Investigatory Powers Commissioner as soon as reasonably practical and no later than 5 working days (or as agreed with the Commissioner) after it has been established by the appropriate internal governance processes that a relevant error has occurred, as this type of occurrence could have significant consequences for the individual whose details were wrongly disclosed.

- **Recordable Errors** are ones where an error has occurred but has been identified before the communications data has been acquired. The Council must keep a record of these occurrences, but a report does not have to be made to the Commissioner.

Reportable Errors could include:

- A notice being made for a purpose, or for a type of data, which the public authority cannot seek;
- Human error, such as incorrect transposition of information;
- Disclosure of the wrong information by a CSP when complying with a notice; or
- Disclosure or acquisition of data in excess of that required.

Recordable Errors could include:

- A notice which is impossible for a Communications Service Provider to comply with;
- Failure to review information already held, e.g. seeking data already acquired or obtained for the same investigation, or data for which the requirement to obtain it is known to be no longer valid;
- Notices being sent out to the wrong CSP; or
- Notices being sent out to CSPs that were not produced by the Approved Rank Officer who authorised the application.

Where a telephone number has been sent to another Telecommunications Operator or Postal Operator, then this does not constitute an error. Where excess data is disclosed, if the material is not relevant to the investigation it should be destroyed once the report has been made to the Commissioner.

If having reviewed the excess material it is intended to make use of it, the Applicant must make an addendum to the original application to set out the reasons for needing to use this excess data. The SRO for Communications Data will then decide whether it is necessary and proportionate for the excess data to be used in the investigation (see paragraphs 24.38 – 24.42 of the Communications Data Code of Practice 2018).

Any reportable error must be reported to the SRO and to the Commissioner within 5 working days. NAFN reports errors on behalf of the Council and the SRO will be made aware of these for the Council's records and any internal action required. If the report relates to an error made by a Telecoms Operators/Postal Operators, it must still be reported, but NAFN shall inform the Telecoms Operators/Postal Operators to enable them to investigate the cause.

The records kept for recordable errors must include details of the error, explain how the error occurred and provide an indication of the steps that will take place to prevent a reoccurrence. These records must be available for inspection by the Investigatory Powers Commissioner inspectors and must be regularly reviewed by the SRO.

Serious Errors

Regarding a 'Serious Error', which 'caused significant prejudice or harm to the person concerned', this must be reported to the Council's SRO the IPC. The IPC may inform the affected individual subject of the data disclosure, who may make a complaint to the IPT. The IPC must be satisfied that the error is a) a serious error AND b) it is in the public interest for the individual concerned to be informed of the error.

Before deciding if the error is serious or not the IPC will accept submissions from the Council as to whether disclosure is in the public interest e.g. it may not be in the public interest to disclose if to do so would be prejudicial to the 'prevention and detection of crime'.

See paragraphs 25.1 – 25.9 of the Communications Data Code of Practice 2018 for more information on the role of the Investigatory Powers Commissioner and 25.10 – 25.17 for more information regarding the role of the Information Commissioner.

See also paragraphs 25.18 – 25.21 of the Communications Data Code of Practice 2018 for further information regarding Enforcement of integrity, destruction and security standards.

Authorising the Acquisition of Communications Data

Section 81 of the IPA 2016 provides a defence if acquisition and disclosure of communications data is challenged:

81. Lawfulness of conduct authorised by this Part
(1) Conduct is lawful for all purposes if—
(a) it is conduct in which any person is authorised to engage by an authorisation or required to undertake by virtue of a notice given in pursuance of an authorisation, and
(b) the conduct is in accordance with, or in pursuance of, the authorisation or notice.

Therefore, to take advantage of this defence, the surveillance needs to be properly authorised.

The Test of Necessity and Proportionality

The acquisition of communications data should only be authorised if the Approved Rank Officer is satisfied that:

1. **The action is NECESSARY on the following grounds:**

    - For the prevention or detection of crime or the prevention of disorder and,

2. **The surveillance is PROPORTIONATE - The Human Rights Act defines a measure or action as proportionate if it:**

    - Impairs as little as possible the rights and freedoms (of the individual concerned and of innocent third parties); and

    - Is carefully designed to meet the objectives in question is not arbitrary, unfair or based on irrational considerations.

Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

An application may contain several requests for various types of data relating to a specific investigation or operation. Consideration should therefore be given as to how this may affect the efficiency of the public authority's processes and the impact of managing disclosure issues before, during and after a criminal trial.

For further guidance, please see the relevant Home Office guidance available from the Home Office website: https://www.gov.uk/government/collections/ripa-codes

Time Limits

The application should specify the shortest period for the data that is necessary in order to achieve the objective for which the data is sought.

All notices and authorisations requesting communications data from the service provider will only be valid for 1 month from the date of granted authorisation/notice given (by the OCDA through NAFN's SPOC). A renewal for a period of up to 1 month can be made and a renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing.

Where the Approved Rank Officer agrees to the renewal, the Approved Rank Officer must have considered the reasons why it is necessary and proportionate to continue, and record the date of the renewal.

Where an authorisation should be cancelled (e.g. no longer necessary or proportionate), NAFN's SPOC must be notified immediately. The SPOC shall cancel the authorised action and take steps to notify the postal or telecommunications service provider without delay.

The Approved Rank Officer

The Approved Rank Officer is the person who is a manager at service level or above within the Council, and their role is to have an awareness of the application made by the Applicant, and confirm this to NAFN's SPOC. They do not authorise or approve the application.

If the Approved Rank Officer having read the application considers the Applicant has met all the requirements for necessity and proportionality then he/she should simply record that fact. A simple note by the Approved Rank Officer should be recorded.

If the Approved Rank Officer does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPOC and the Applicant.

Similarly, if a Magistrate rejects an application, the application should be rejected and referred back to the SPOC.

If the application is rejected either by the SPOC or the Approved Rank Officer, the SPOC will retain the form and inform the applicant in writing of the reasons for its rejection. The NAFN's SPOC will do so via the website.

If the Approved Rank Officer is recording their considerations within the NAFN database and is attributable to the Approved Rank Officer, a signature is not required.

The Central Register of Authorisations – Communications Data

In respect of communications data, NAFN's SPOC will retain copies of the original of all applications, authorisations, copies of notices and withdrawals of authorisations and cancellation of notices, cross-referenced against each associated document.

Applications, authorisations, copies of notices, and records of the withdrawal and cancellation of authorisations, must be retained in written or electronic form for a minimum of 3 years. A record of the date and, when appropriate, the time each notice or authorisation is granted, renewed or cancelled (see paragraphs 24.1-24.9 of the Communications Data Code of Practice for full details of the level of information that should be retained).

Nothing in this Policy has an affect on similar duties under the Criminal Procedure and Investigations Act 1996, which requires material obtained in the course of an investigation and that may be relevant to the investigation to be recorded, retained and revealed to the prosecutor.

When the NAFN system is being used, the retention of documents service will be provided by NAFN, who shall also provide copies periodically, and as requested, to the SRO for Communications Data, and deal with any requests from inspectors from the ICO.

Nonetheless, the Council's Central Record should also contain a record of:

- Number of applications rejected by Approved Rank Officer;
- Number of notices requiring disclosure of communications data within the meaning of each subsection of Section 21(4);
- Number of authorisations for acquiring of communications data within the meaning of each subsection of Section 21(4); and
- Number of times an urgent notice is given orally.

NAFN are able to provide on request, statistical information about the numbers of notices or authorisations that they have issued on behalf of the Council during a particular time period including any errors that have occurred. The Council's SRO for Communications Data will request such information from NAFN on a quarterly basis.

COMPLAINTS

As set out in paragraph 26.2 of the Communications Data Code of Practice 2018, **t**he Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the Act. Failure to comply with the provisions of the Communications Data Code of Practice 2018 in these areas may also engage concerns about compliance with data protection and related legislation. Any concerns about compliance with data protection and related legislation should be passed to the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
0303 123 1113
www.ico.org.uk

As set out in paragraph 26.3 of the Communications Data Code of Practice 2018, the Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers, including those covered by this code, as well as conduct by or on behalf of any of the intelligence services and is the only appropriate tribunal for human rights claims against the intelligence agencies. Any complaints about the use of powers as described in this code should be directed to the IPT.

Any individual who is dissatisfied about the way the Council has or is carrying out surveillance may make a complaint. The decision as to which procedure should be used lies with the individual concerned.

If a person wishes to complain using the Council's procedures, then the complainant should be made aware of the Council's Corporate Complaints Procedure (see https://www.ceredigion.gov.uk/your-council/comments-compliments-and-complaints/corporate-complaints/ and https://www.ceredigion.gov.uk/media/1179/complaints-policy-bookletenglish.pdf) The complaint will be dealt with in accordance with that procedure.

If a person wishes to complain directly to an independent body or had used the Council's internal procedures and is still dissatisfied, then he/she may complain to the Investigatory Powers Tribunal ('IPT').

The IPT has jurisdiction to investigate and determine complaints against public authority use of investigatory powers. To find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com.

Complaints can be made in writing to:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

* See Part 4 above for complaints regarding Directed Surveillance or a CHIS.

PART 6 - Non-RIPA Surveillance

Meaning of 'non-RIPA Surveillance'

From time to time, the Council may wish to undertake covert surveillance, which is not regulated by RIPA. This is fine, as RIPA is permissive legislation. The procedures and guidance below sets out the processes required for NON-RIPA authorisation. The process is in intended to reflect that of a RIPA authorisation, save for the judicial approval requirement. More information is contained below outlining the procedures to be followed in respect of Non-RIPA Surveillance, including the completion of an application form.

It is important to have a procedure in place for non-RIPA Surveillance, as mechanisms for activity, which cannot be protected is encouraged. In those circumstances, statutory definitions are met but not under the RIPA grounds. The human rights aspects must still be considered and an authorisation provides a useful audit of decisions and actions.

Investigating officers are required to obtain a Unique Reference Number ('URN') from the SRO prior to submission to an Authorising Officer for non-RIPA Surveillance.

Authorisation under RIPA affords the Council a defence under S.27 of RIPA i.e. the activity is lawful for all purposes, provided an authorisation is in place, and the conduct of the Officers is in accordance with the legislation. However, failure to obtain an authorisation does not make covert surveillance unlawful.

RIPA is a shield not a sword and Section 80 of RIPA contains a general saving for lawful conduct:

'Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or notice, or by virtue of which information may be obtained in any manner, shall be construed –

(a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;
(b) as otherwise requiring—
(i) the issue, grant or giving of such a warrant, authorisation or notice, or
(ii) the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice, before any such conduct of that description is engaged in; or
(c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act.'

This point was explained more fully by the Investigatory Powers Tribunal in the case of C v The Police (Case No: IPT/03/32/H 14th November 2006):

'Although RIPA provides a framework for obtaining internal authorisations of directed surveillance (and other forms of surveillance), there is no general prohibition in RIPA against conducting directed surveillance without RIPA authorisation. RIPA does not require prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful.'

Why carry out non-RIPA Surveillance?

The Council may wish to do such '*non-RIPA Surveillance*' for one of two reasons:

I. Crimes Not Carrying Six Months of Imprisonment

As stated above, the Council's AOs may not authorise Directed Surveillance under RIPA unless it is for the purpose of preventing or detecting a criminal offence, and it meets the condition set out in New Article 7A (3)(a) or (b) of the 2010 Order. Those conditions are that the criminal offence sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a term of **at least 6 months of imprisonment**, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (offences involving sale of tobacco and alcohol to underage children).

However, just because a crime does not meet the six-month test does not mean covert surveillance cannot be undertaken.

This point was made by the Chief Surveillance Commissioner in his annual report (2010/2011):

'The higher threshold in the proposed legislation will reduce the number of cases in which local authorities have the protection of RIPA when conducting covert surveillance; it will not prevent the use of those tactics in cases where the threshold is not reached but where it may be necessary and proportionate to obtain evidence covertly and there will be no RIPA audit trail. Part I of RIPA makes unauthorised interception unlawful. In contrast, Part II makes authorised surveillance lawful but does not make unauthorised surveillance unlawful.'

II. Employee Surveillance

Most employee surveillance will not be able to be authorised under RIPA.

See the previous decision by the Investigatory Powers Tribunal: C v The Police and the Secretary of State for the Home Department (14th November 2006, No. IPT/03/32/H)

C, a former police sergeant, retired in 2001 having made a claim for a back injury he sustained after tripping on a carpet in a police station. He was awarded damages and an enhanced pension due to the injuries.

In 2002, the police instructed a firm of private detectives to observe C to see if he was doing anything that was inconsistent with his claimed injuries. Video footage showed him mowing the lawn. C sued the police claiming they had carried out directed surveillance without an authorisation. The Tribunal first had to decide if it had jurisdiction to hear the claim. The case turned on the interpretation of the first limb of the definition of directed surveillance i.e. was the surveillance 'for the purposes of a specific investigation or a specific operation?'

The Tribunal ruled that this was not the type of surveillance that RIPA was meant to regulate. It made the distinction between the ordinary functions and the core functions of a public authority:

'The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers.'

The Tribunal also stated that it would not be right to apply RIPA to such surveillance for a number of reasons:

1) RIPA does not cover all public authorities, and there was no sense in police employee surveillance being conducted on a different legal footing than, for example, the Treasury, which does not have the same surveillance rights under RIPA.
2) The Tribunal has very restrictive rules about evidence, openness and rights of appeal. The effect of these would lead to unfairness for employees of RIPA authorities when challenging their employers' surveillance as compared to those who were employed by non-RIPA authorities.

This case suggests that, even where employee surveillance is being carried out on one of the grounds in section 28(3), the key question is:

Is it for a core function linked to one of the authority's regulatory functions? Within a local authority context, this would include, amongst others, Trading Standards, Environmental Health and Licensing. If it is not being done for one of these purposes, it will not be directed surveillance.

Online covert activity-Internet and Social Networking Sites ('SNS')

See the Council's RIPA Social Media Policy for guidance regarding on-line covert activity regarding the Internet and SNS, which must be read in conjunction with this Policy.

*See **Flowchart 9 –Authorising Non-RIPA Surveillance***

Human Rights Legislation Compliance

Covert surveillance done without a RIPA authorisation will not have the protection of RIPA (i.e. the defence in S.27 of RIPA). However, it will still be able to be undertaken as long as it is done in accordance with the ECHR, which is directly enforceable against public authorities pursuant to the Human Rights Act 1998, as stated above.

Article 8 of the ECHR states:
'Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the rights and freedoms of others.'

To satisfy Article 8 ECHR, the covert surveillance must be **both necessary and proportionate**. In deciding whether it is, the same factors need to be considered as when authorising surveillance regulated by RIPA.

Data Protection Legislation Compliance

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) ('the Telecommunications Regulations) permit the Council without further authorisation to lawfully intercept its employees email or telephone communications, and also to monitor their internet access for purposes of prevention or detection of crime, or the detection of unauthorised use of these systems. Regard should be

had to the Council's Internal Information Security Policy (available on the Council's Intranet Site (Cerinet).

Further advice on these regulations should be sought from the Council's Data Protection Officer and regard should be had to the Council's internal Information Security Policy, and also the '*ICO Quick Guide to the Employment Practice Code'* (see https://ico.org.uk/media/for-organisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf).

When doing covert surveillance of employees not regulated by RIPA, the Data Protection Act 1998 ('DPA') will apply, as personal information about living individuals will be being processed e.g. their movements, photographs etc.

The Information Commissioner has published a Data Protection Employment Practices Code of Practice (available at www.ico.gov.uk). This type of surveillance is outside the remit of this document.

In both the above cases, it is important to have a proper audit trail through written records.

Data Protection Employment Practices Code of Practice

The Information Commissioner has published a **Data Protection Employment Practices Code of Practice** (available at: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf (the 'DPEP Code') Part 3 of the DPEP Code covers all types of employee surveillance from video monitoring and vehicle tracking to email and internet surveillance. It gives guidance on how to do employee surveillance in a way that complies with the DPA. Whilst the code is not law, it can be taken into account by the Information Commissioner and the courts in deciding whether the DPA has been complied with.

The DPEP Code states that employee monitoring should take place for a clear justified purpose and employees should be aware that it is taking place.

With regard to covert surveillance, it states that it will be rare for such monitoring to be justified. It should therefore only be used in exceptional circumstances e.g. prevention or detection of crime or serious malpractice.

One of the other main recommendations of the DPEP Code is that senior management should normally authorise any covert monitoring of employees. They should satisfy themselves that there are grounds for suspecting criminal activity or equivalent malpractice. They should carry out an impact assessment and consider whether the surveillance is necessary and proportionate to what is sought to be achieved.

The DPEP Code sets out other rules that local authorities (and others) need to consider when doing covert surveillance of employees:

- Prior to the investigation, clear rules must be set up limiting the disclosure and access to information obtained;
- The number of people involved in a covert monitoring exercise should be limited;
- The surveillance must be strictly targeted at obtaining evidence within a set time frame and it should not continue after the investigation is complete;
- If using audio or video equipment, this should not normally be used in places such as toilets or private offices;

- Information obtained through covert monitoring should only be used for the prevention or detection of criminal activity or serious malpractice; and
- Other information collected in the course of monitoring should be disregarded and, where feasible, deleted unless it reveals information that no employer could reasonably be expected to ignore.

In both the above Non-RIPA cases, it is important to have a proper audit trail through written records. In his annual report (2011/2012), the Chief Surveillance Commissioner (at paragraph 5.22) emphasised this:

'I occasionally encourage the use of similar authorisation mechanisms for activity which cannot be protected by the Acts (for example where covert techniques are used to identify a missing person when no crime is suspected). In these circumstances statutory definitions are met but none of the grounds specified in RIPA section 28(3) or RIP(S)A section 6(3), yet the human rights of the subject of surveillance must be considered. The authorisation process provides a useful audit of decisions and actions.'

Authorising Officers for non-RIPA Surveillance

The Authorising Officers for non-RIPA Surveillance are the same Authorising Officers as authorise RIPA Surveillance i.e.:

- **Corporate Lead Officer: People and Organisation;**
- **Corporate Lead Officer: Policy, Performance & Public Protection; and**
- **Corporate Lead Officer: Porth Cynnal.**

Similar mechanisms for activity which cannot be protected by RIPA legislation is encouraged. In those circumstances, statutory definitions are met, but not under the grounds specified in RIPA. The human rights aspects must still be considered. An authorisation process provides a useful audit of decisions and actions. The process reflects that of directed surveillance, save for the Judicial Approval requirement.

A URN should be sought from the Senior Responsible Officer prior to submission to Authorising Officers, with the original form sent to the SRO for entry in the Central Register upon completion of authorisation process, and a copy retained by the Service.

Non-RIPA Surveillance Authorisation Form

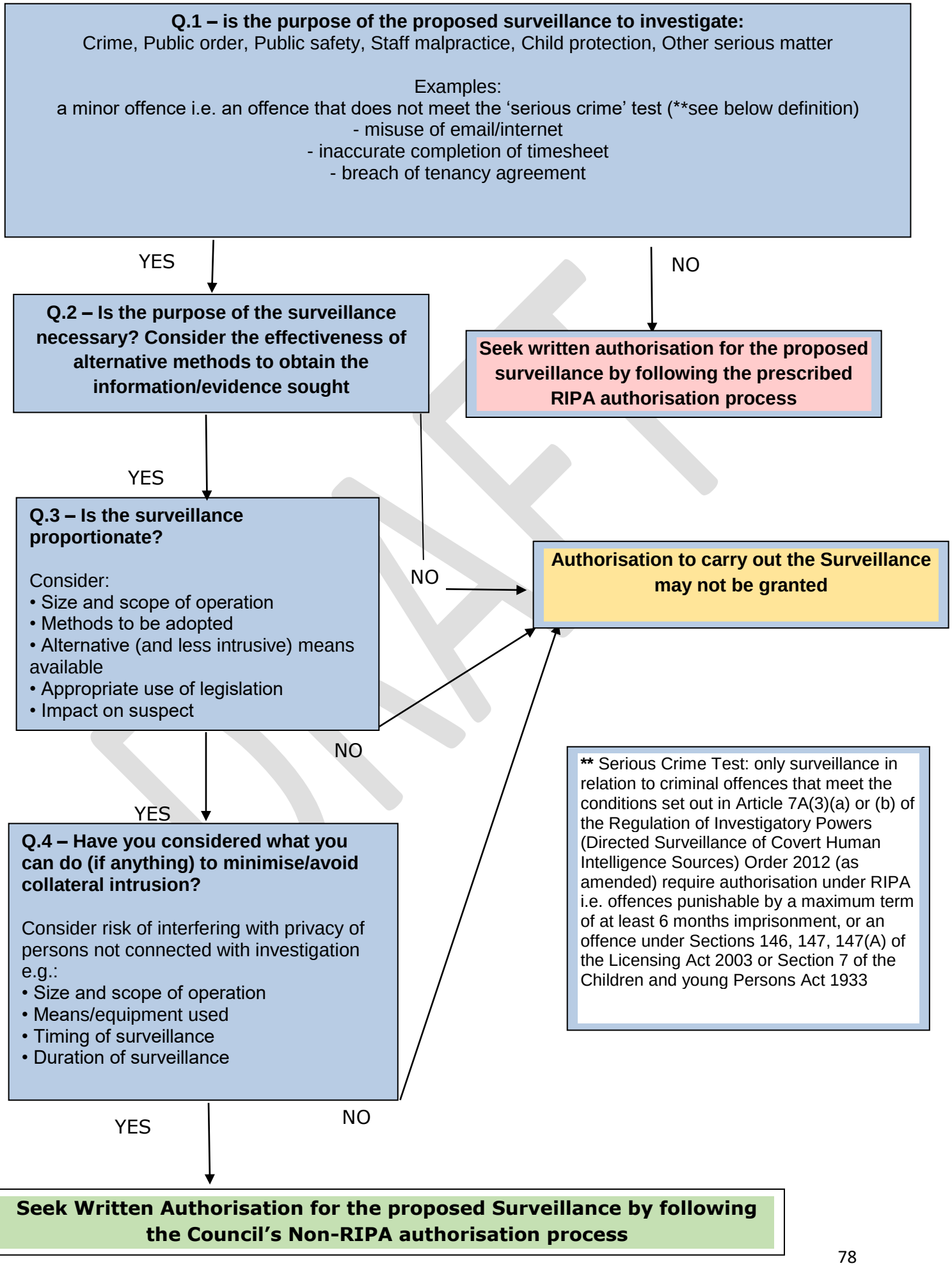
A Non-RIPA authorisation form must be completed, as above, and an example form with guidance is available on the Council's intranet site (CeriNet) at [enter link].

Lifecycle of a Non-RIPA surveillance authorisation

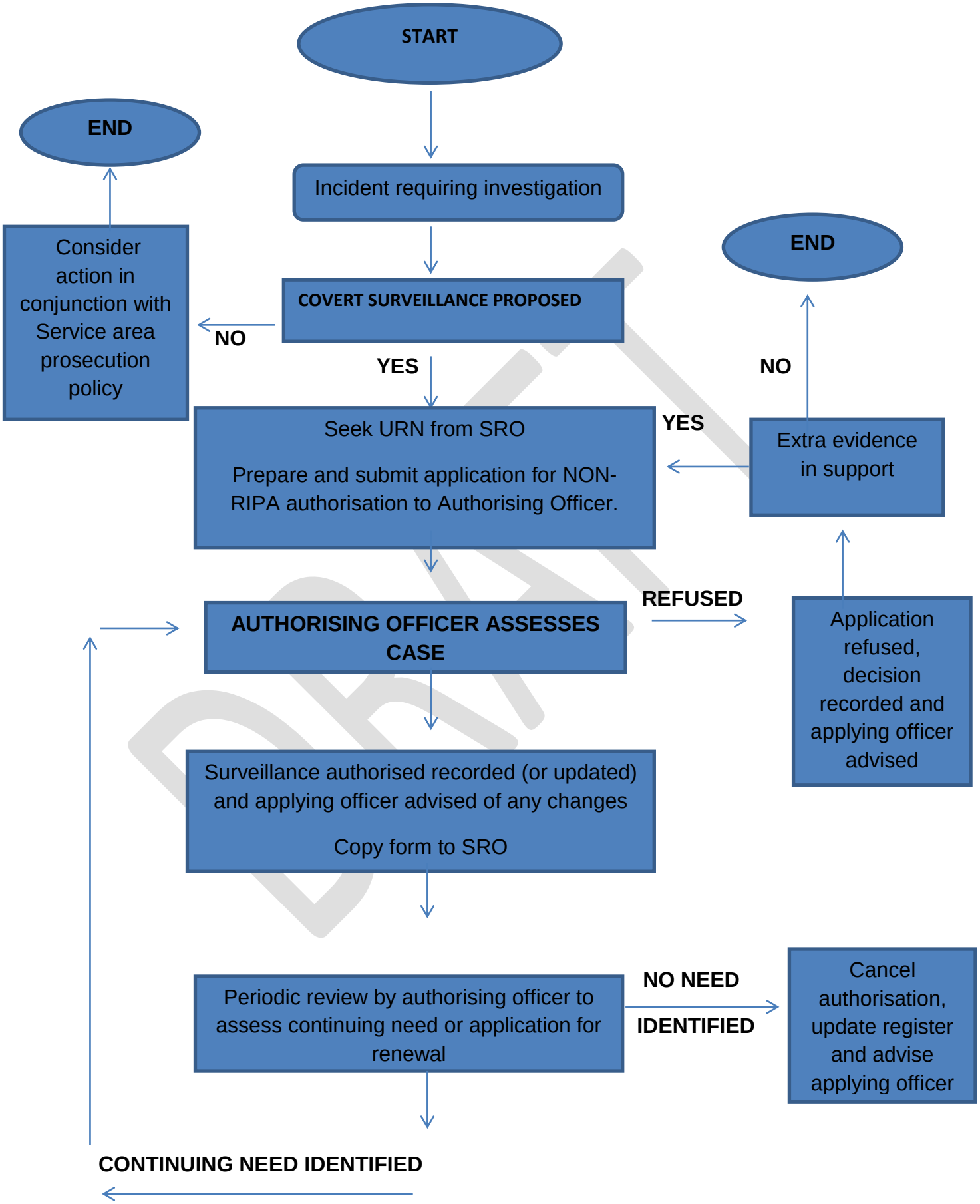
A Flowchart showing the basic lifecycle of a Non-RIPA surveillance authorisation is shown below**.** This is identical to the lifecycle for Directed RIPA Surveillance, except that judicial approval is not required.

Non-RIPA activity will be reported to the Overview & Coordinating Scrutiny Committee.

Flowchart 9- Authorising Non-RIPA Surveillance



Flowchart 10 – Non RIPA Surveillance - Basic Lifecycle of a Directed Surveillance Authorisation



Schedule 1 – Relevant Legislation, Codes of Practice, Policies & Guidance

The Ceredigion County Council RIPA Corporate Policy and Procedures Document should be read in conjunction with all current and relevant legislation, guidance and codes of practice, including (but not limited to) the following:

- The Regulation of Investigatory Powers Act 2000
  http://www.legislation.gov.uk/ukpga/2000/23/contents
- RIPA Explanatory Notes
  http://www.legislation.gov.uk/ukpga/2000/23/notes/contents

- RIPA Statutory Codes of Practice:
  - Covert Surveillance and Property Interference Revised Code of Practice 2018
    https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf
  - Covert Human Intelligence Sources Revised Code of Practice
    https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf
  - Bulk Acquisition of Communications Data Code of Practice:
    https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf
  - Communications Data Code of Practice 2018:
    https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf
  - Investigation of Protected Electronic Information Revised Code of Practice
    https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742064/RIPA_Part_III_Code_of_Practice.pdf
  - Equipment interference Code of Practice 2018
    https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf

- Investigatory Powers Act 2016 ('IPA 2016')
  https://www.legislation.gov.uk/ukpga/2016/25/contents

- SI 2010 N0.521 - Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
  http://www.legislation.gov.uk/uksi/2010/521/contents/made
- SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012)
  http://www.legislation.gov.uk/uksi/2012/1500/contents/made

- Guidance issued by the Investigatory Powers Commissioner's Officer ('IPCO') (formerly the Office of Surveillance Commissioner ('OSC') (available at: https://www.ipco.org.uk/) including OSC Procedures and Guidance Document:
  https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/OSC-PROCEDURES-AND-GUIDANCE.pdf

- Information Commissioner's Office Data Protection Employment Practices Code
  https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

- Home Office Surveillance Camera Code of Practice (2013)

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

- The Council's Social Media Policy: https://ceri.ceredigion.gov.uk/portal/employee-handbook/policies-procedures/social-media-policy/

- The Council's Information Security Policy; https://www.ceredigion.gov.uk/your-council/strategies-plans-policies/information-security-policy/

- The Council's Code of Conduct for Local Government Employees*

- The Council's Data Protection and GDPR Policy**

- The Council's Email Policy*

- The Council's Information and Records Management Policy (available at https://www.ceredigion.gov.uk/your-council/strategies-plans-policies/information-and-records-management-policy/)**

- The Council's Policy and Guidelines for Safeguarding Children & Adults at Risk*

- The Council's Social Media Editorial and Administration Policy*

- The Council's Whistleblowing Policy*

*: available on the Council's intranet site (CeriNet)
**: available on the Council's website and CeriNet