

ROTHERHAM BOROUGH COUNCIL

RIPA Policy

July 2023

INDEX

1.	Covert Surveillance Policy Statement	Page 3
2.	Guide to Surveillance Regulated by Part 2 of RIPA	Page 5
	i) Directed Surveillance	Page 6
	ii) Intrusive Surveillance	Page 12
	iii) CHIS	Page 15
3.	Guidance for Authorising Officers	Page 20
4.	Seeking Magistrates' Approval	Page 32
5.	Notes to Assist Completion - Magistrates Approval	Page 39
6.	Governance Arrangements & Quality Assurance	Page 41

ROTHERHAM BOROUGH COUNCIL

1. COVERT SURVEILLANCE POLICY STATEMENT

Introduction

1. Rotherham Borough 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. The Council shall ensure that covert surveillance is only undertaken where it complies fully with all applicable laws in particular the:-
 - Human Rights Act 1998
 - Regulation of Investigatory Powers Act 2000 (“RIPA”)
 - Protection of Freedoms Act 2012
 - Data Protection Act 2018
6. The Council shall, in addition, have due regard to all official guidance and codes of practice particularly those issued by the Home Office, the Investigatory Powers Commissioner’s Office, the Surveillance 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 out covert surveillance shall be granted by appropriately trained and designated authorising officers. A list of those authorising officers who have been nominated by their Directorate and have undertaken appropriate training is held by the Senior Responsible Officer (SRO).
- Covert surveillance which is regulated by RIPA shall only be undertaken after obtaining judicial approval.
- The operation of this Policy and Procedure will be overseen by the SRO, whose role is described later in this document.

Training and Review

8. All Council officers undertaking and authorising covert surveillance shall be appropriately trained to ensure that they understand their legal and moral obligations.
9. Quality Assurance checks shall be carried out by the Solicitor with conduct of a specific case and the RIPA Co-ordinator to ensure that officers are complying with this policy when the authorisation forms are forwarded to Legal Services for the Judicial Approval applications. All other forms – Renewals, Review, and Cancellation forms are submitted to the RIPA Coordinator who will collate the forms for the Central Record.
10. This policy shall be reviewed at least once a year in the light of the latest legal developments and changes to official guidance and codes of practice.
11. The operation of this policy shall be overseen by the Council's Audit Committee by receiving reports on a 12 monthly basis to ensure that the RIPA powers are being used consistently with this policy.

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. An electronic copy of this Policy can be found on the Council's Intranet on the Key Documents section of the Legal Services page.
15. Any questions relating to this policy should be addressed to:

Contact: Phil Horsfield, Assistant Director for Legal Services (Senior Responsible Officer) – 01709 254437

Bal Nahal, Head of Legal Services (RIPA Coordinator) – 01709 823661

Michelle Scales, Senior Solicitor for Litigation – 01709 823145

2. GUIDE TO SURVEILLANCE REGULATED BY PART 2 OF RIPA

Part 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 European Convention of Human Rights (ECHR), particularly Article 8, the right to respect for private and family life. The purpose of this part of the procedure is to help you decide what type of surveillance you are doing and whether it is regulated by Part 2.

The Law

- 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>
- Covert Surveillance and Property Interference Statutory Code of Practice (Revised August 2018)
<https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice>
- Covert Human Intelligence Sources Statutory Code of Practice [Revised December 2022]
<https://www.gov.uk/government/publications/covert-human-intelligence-sources-code-of-practice-2022>
- 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/pdfs/uksi_20100521_en.pdf
- 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/pdfs/uksi_20121500_en.pdf

The Surveillance Techniques which Local Authorities may authorise

Part 2 of RIPA allows local authorities to authorise two out of the three techniques it regulates i.e. the use of directed surveillance and covert human intelligence sources. The first issue for any local authority officer, considering undertaking covert surveillance is: **is it something that can be authorised under RIPA?**

Let us consider the definitions of the different types of surveillance regulated by Part 2 of RIPA:

1. Directed Surveillance

2. Intrusive Surveillance
3. Covert Human Intelligence Source (CHIS)

i) Directed Surveillance: This is defined in S.26(2) of the Act:

“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 serious environmental crime 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) six questions before the activity can be classed as Directed Surveillance:

- Is the surveillance, actually “surveillance” as defined by the Act?
- 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 an immediate response to events?

Please consult Flowchart 1 when deciding if your surveillance is Directed.

Key Points to Note

1. General observations do not constitute Directed Surveillance. The Covert Surveillance Code (para 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.”

2. Surveillance is only Directed if it is covert. S.26(9)(a) states:

“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.

3. The definition of “private information” is very wide. The Covert Surveillance and Property Interference Code at paragraphs 3.3 to 3.6 states:

3.3 *The 2000 Act states that private information includes any information relating to a person’s private or family life¹⁰. As a result, private information is capable of including any aspect of a person’s private or personal relationship with others, such as family¹¹ 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 available 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.¹² 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. See paragraphs 3.10 to 3.17 below for further guidance about the use of the internet as a surveillance tool.*

3.5 *Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.*

3.6 *Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.*

4. Where covert surveillance needs to be done in an emergency and there is no time (or no Authorising Officer available) to authorise the activity, the surveillance can still be done. It will not constitute Directed Surveillance. The Covert Surveillance Code (para 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.”

5. If the Council authorises a non-employee (e.g. an enquiry agent) to conduct covert surveillance then that person/company is acting as an agent for the Council. The Authorising Officer must ensure that the person/company is competent and they have provided a written acknowledgment that they are an agent of the Council and will comply with the authorisation.
6. The revised Code of Practice for Covert Surveillance and Property Interference at paragraphs 3.10 to 3.17 clarifies the position on the use of social media for surveillance and provides examples:

3.10 *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 authorisation; 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.*

- 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.

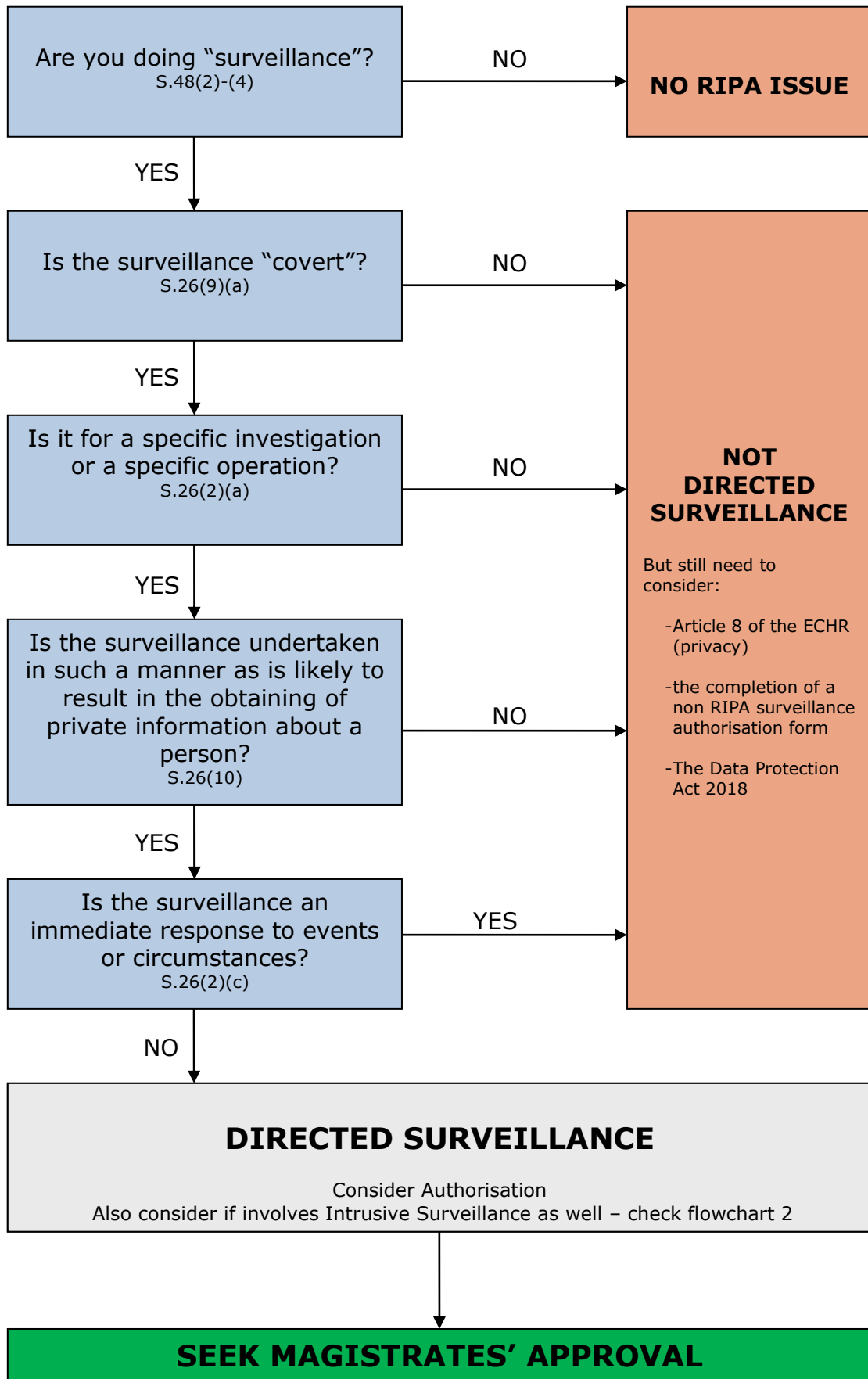
3.16 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should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

No officer should make repeated visits to the same open source social media site as part of an investigation unless they have first spoken to the Assistant Director for Legal Services (Phil Horsfield 01709 254437), the Council's RIPA Coordinator, the Head of Legal Services (Bal Nahal 01709 823661) or the Senior Solicitor for Litigation (Michelle Scales 01709 823145) to ensure that it is lawful to do so.

Flowchart 1 - Are you conducting Directed Surveillance?



ii) **Intrusive Surveillance:** S.26(3) 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 the Act or by a member or official of those public authorities listed in or added to section 41(l). **Local authorities are not listed therein and so cannot authorise such Intrusive Surveillance.**

It is still important for investigating officers to understand the definition of Intrusive Surveillance in order for them to be able to ensure that Directed Surveillance does not inadvertently extend into Intrusive Surveillance. The following issues should be considered in each case:

- Is it Covert Surveillance as defined by the Act?
- 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?
- Is it being carried out by means of a surveillance device on the premises or in the vehicle?

Please consult Flowchart 2 when deciding if your surveillance is Intrusive.

Key Points to Note

1. 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):

“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);”

Environmental health officers doing covert surveillance of takeaways, restaurants and shops will not be doing Intrusive Surveillance. Care must be taken though where a shop also contains living quarters and covert filming may capture images of people in those quarters. Other examples of residential premises include flats, hotel rooms, caravans and even boats, which are used as living quarters. Care must be taken in such situations to avoid the accusation that unauthorised Intrusive Surveillance was carried out.

2. 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 chauffer driven vehicle such as a public coach service.

3. For the surveillance to be Intrusive rather than just Directed it has got 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. This could only be conceivably done if the investigating officer hides in the boot of the target vehicle!

However, it may be that an officer is stationed inside residential premises to covertly observe drug dealing or 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 jump over the fence and hide in the garden to obtain clearer images.

4. 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.

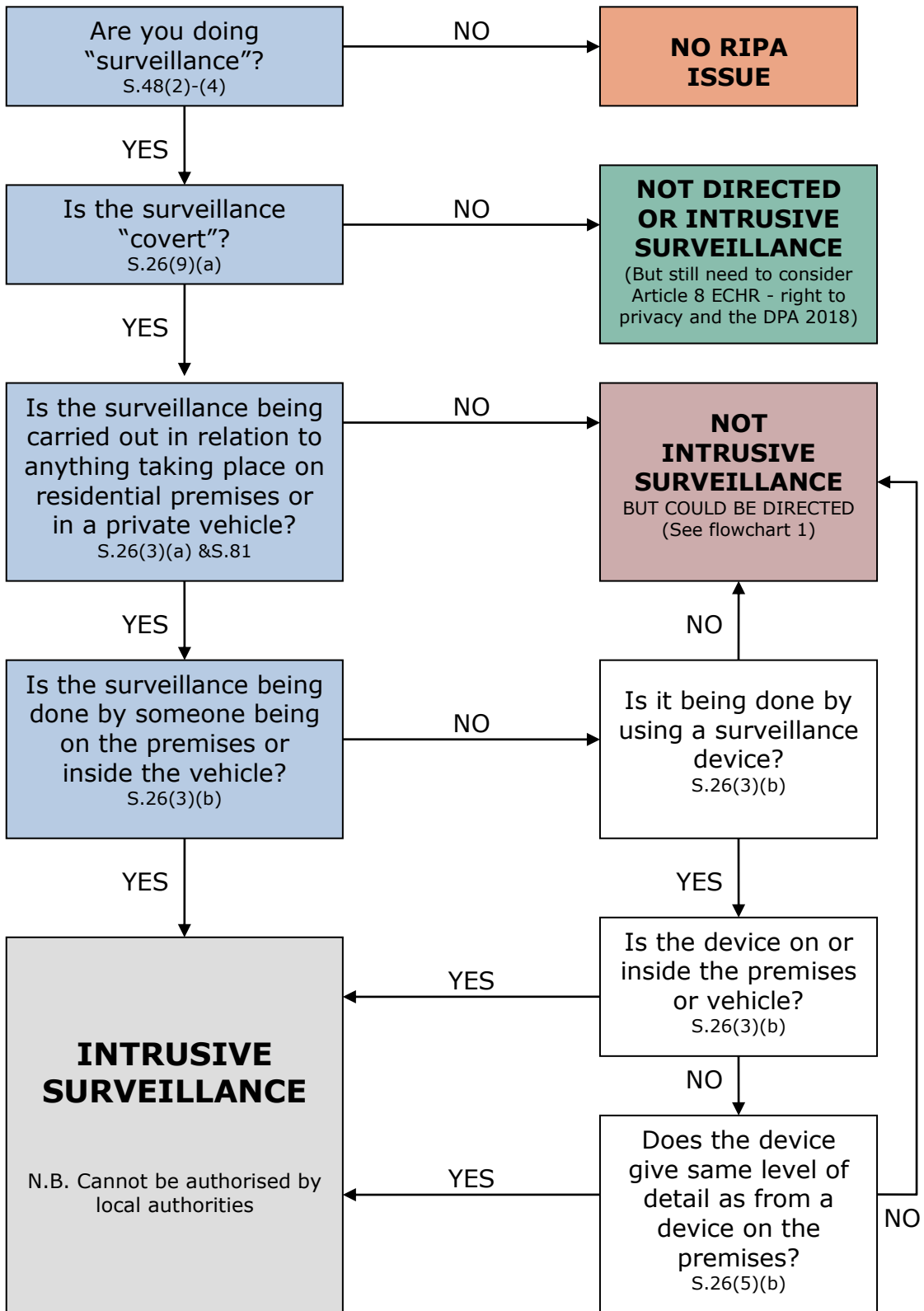
However, the words of S.26 (5) should be noted:

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?



iii) **A Covert Human Intelligence Source (CHIS)** This is defined in S.26(8):

“...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:

- Is the person establishing or maintain a personal or other relationship with a person?
- Is that relationship being used for a covert purpose?
- Is the covert purpose facilitating the doing of anything falling within paragraph (b) or (c) (above)?

Please consult Flowchart 3 when deciding if your 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.

Key Points to Note

1. A public volunteer is not a CHIS. The CHIS code (para 2.21) states:

“In many cases involving human sources, the source will not have established or maintained a relationship for a covert purpose. Many sources provide information that they have observed or acquired other than through a relationship. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation is required.”

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

2. 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.
3. A test purchaser, though technically a CHIS, may not always require authorisation. Please consult the CHIS Code and the OSC Procedures and Guidance Document for further guidance.

4. The revised Code of Practice for Covert Human Intelligence Sources at paragraphs 4.29 to 4.35 clarifies the position on the use of social media in a potential CHIS context and provides examples:

4.29 *Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation. This applies whether the interaction involves publicly open websites such as online news and social networking service, or more private exchanges such as messaging sites. Where the activity is likely to result in obtaining private information but does not amount to establishing or maintain a CHIS relationship, consideration should be given for a directed surveillance authorisation.*

4.30 *Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:*

- *An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person.*
- *Directing a member of the public to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.*
- *Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.*

4.31 *A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required. However, consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met*

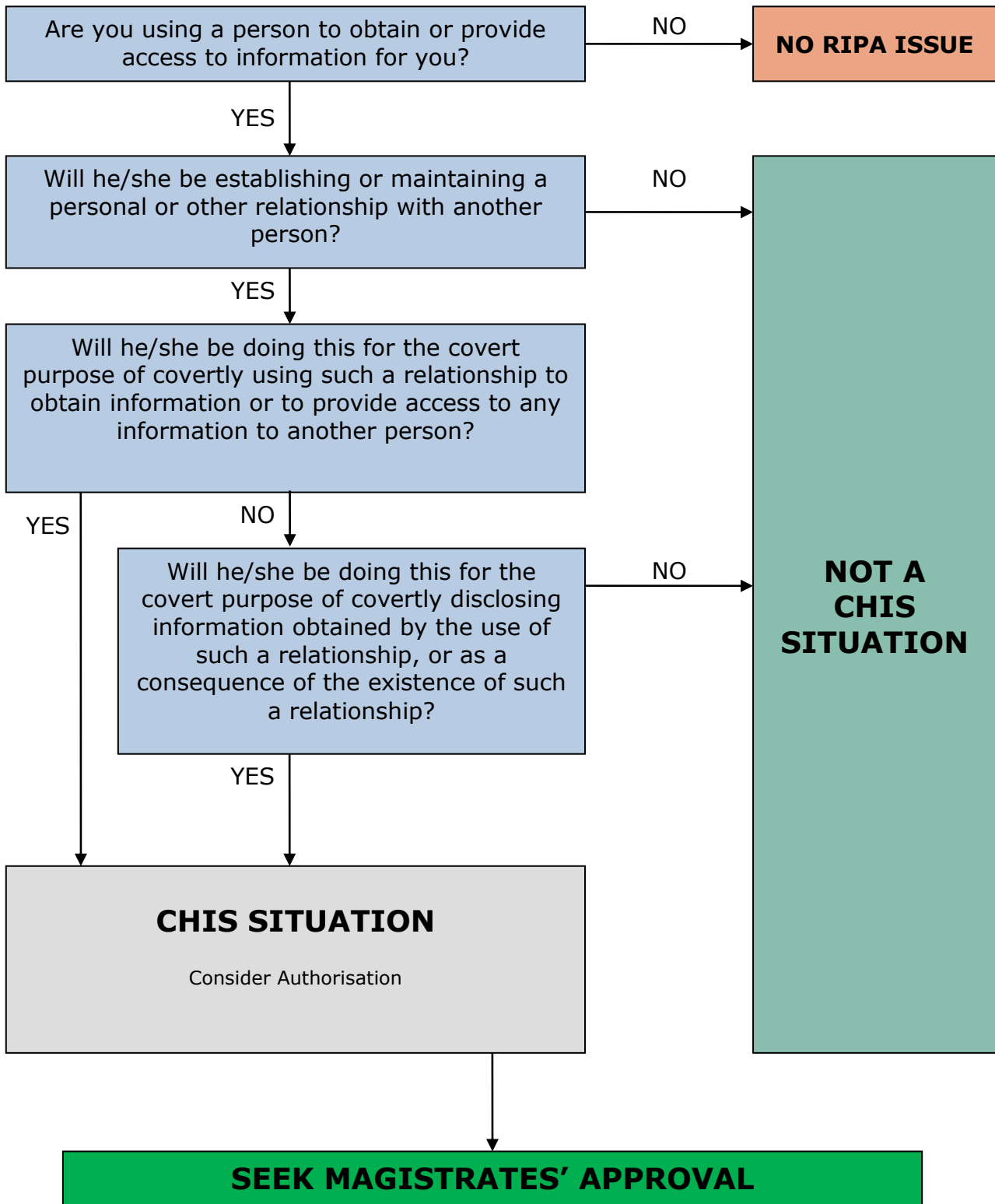
4.32 *Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic*

gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if there is an intention to engage in such interaction to obtain, provide access to or disclose information.

- 4.33 *When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for a CHIS authorisation. Full consideration should be given to the potential risks posed by that activity.*
- 4.34 *Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 7.15 to 7.21 of this code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.*
- 4.35 *Where it is intended that more than one officer will share the same online persona, each individual should be clearly identifiable within the overarching authorisation for that operation. The authorization should provide clear information about the conduct required of - and the risk assessments in relation to - each officer involved. (See also paragraph 3.32 to 3.26)*

No officer should make repeated visits to the same open source social media site as part of an investigation unless they have first spoken to Assistant Director for Legal Services (Phil Horsfield 01709 254437), the Council’s RIPA Coordinator, the Head of Legal Services (Bal Nahal 01709 823661) or the Senior Solicitor for Litigation (Michelle Scales 01709 823145) to ensure that it is lawful to do so.

Flowchart 3 - Are you deploying a CHIS?



Completing the Forms

Once it is decided what type of surveillance is being undertaken, the appropriate form must be completed and sent to the Authorising Officer for approval. Templates of each form together with notes to assist completion and precedent wording are on the Intranet in the same section on the same page as this Policy (Legal Services, Key Documents). It should be noted that as a result of the changes made by the Protection of Freedoms Act 2012, local authorities no longer have the power to make urgent oral authorisations. Therefore, all authorisations, even if urgent, must be made in writing and the relevant judicial approval must be sought.

The Authorising Officer

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 N0.521) states that the Authorising Officer for a local authority can be a Director, Head of Service, Service Manager or equivalent. A list of the Council's Authorising Officers is held by the SRO. All authorising officers will be nominated by their Directorates, as being of sufficient rank and having undertaken appropriate RIPA training. Once the SRO is satisfied that this is the case they will be added to the list of Authorising officers, held by the SRO.

Where the surveillance involves the likelihood of obtaining confidential information or the deployment of juveniles or vulnerable people, then the authorisation has to be sought from the Head of Paid Service or, in his/her absence, the acting Head of Paid Service.

Time Limits

The current time limits for an authorisation are 3 months for Directed Surveillance and 12 months for a CHIS (1 month if the CHIS is underage), from the date of the Magistrate's approval.

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.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire 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).

3. GUIDANCE FOR AUTHORISING OFFICERS

AUTHORISING DIRECTED SURVEILLANCE: RULES AND CRITERIA

Section 27 of RIPA provides a powerful 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.

The Authorising Officer

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010 N0.521) states that the Authorising Officer for a local authority can be a Director, Head of Service, Service Manager or equivalent. As stated above, a list of the Council's approved Authorising Officers is held by the SRO. A list of the current Authorising Officers is set out in section 6.

Where the surveillance involves the likelihood of obtaining confidential information or the deployment of juveniles or vulnerable people, then the authorisation has to be sought from the Head of Paid Service or, in his/her absence, the acting Head of Paid Service.

Time Limits

The current time limits for an authorisation are 3 months for Directed Surveillance and 12 months for a CHIS (1 month if the CHIS is underage), from the date of the Magistrates' approval.

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.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire 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 Consideration (Chapter 3, Covert Surveillance Code)

S.28(2) 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.”

Please consult Flowchart 4 when deciding whether Directed Surveillance should be authorised.

The first question that the Authorising Officer needs to ask is: Is the surveillance necessary? Namely, is it necessary to use directed surveillance in the operation.

The surveillance has to be necessary on one of the grounds set out within 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.

From 1st November 2012, local authority Authorising Officers may not authorise Directed Surveillance 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 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 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.

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

The second question is: 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.

The Investigatory Powers Commissioner Office often states in its inspection reports that officers have not properly understood this concept or have not demonstrated compliance within the authorisation form. The Covert Surveillance Code (para 4.7) 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;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

The third question is; can we avoid or minimise collateral intrusion?

The Authorising Officer 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.

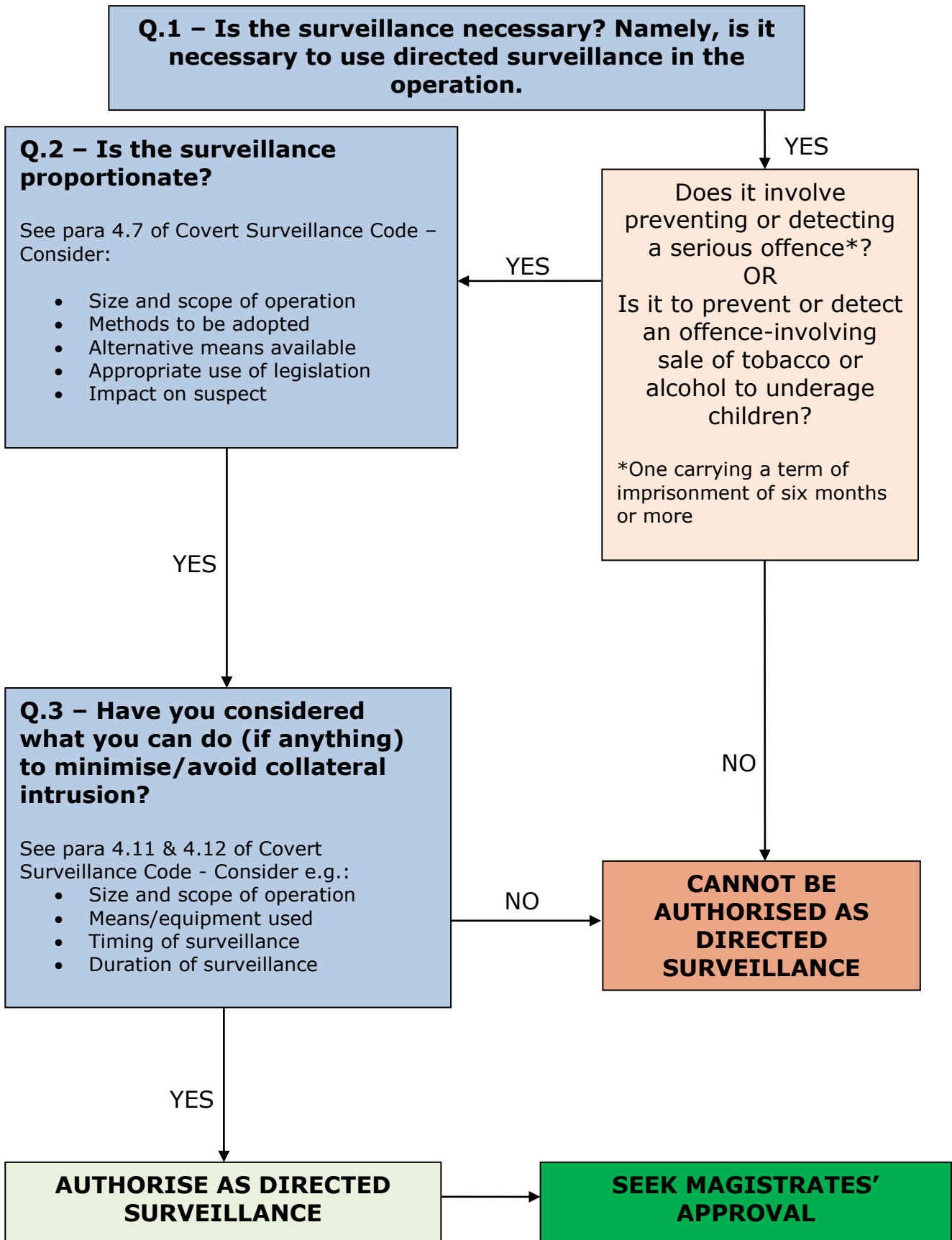
Investigating and Authorising Officers will need to ask themselves:

- What is the impact on third parties? Is it significant?
- If it is, what can be done to avoid or minimise it?
- Have we considered:
 - Changing the timing of the surveillance
 - Reducing the amount of surveillance
 - Changing the method of surveillance
 - The sensitivities of the local community

Surveillance operations by other public authorities - Of course at all times the need to obtain the best evidence to investigate the crime will be paramount.

Next Stage: Once the surveillance has been authorised the next stage is to seek Magistrates' approval. See Section 4 for a detailed explanation of the procedure

Flowchart 4 - Authorising Directed Surveillance



AUTHORISING A CHIS: RULES AND CRITERIA

Section 27 of RIPA provides a powerful 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.

The Authorising Officer

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

Where the surveillance involves the likelihood of obtaining confidential information or the deployment of juveniles or vulnerable people, then the authorisation has to be sought from the Head of Paid Service or, in his/her absence, the acting Head of Paid Service. A list of the Council's Authorising Officers is held by the SRO.

If there is any doubt regarding sufficiency of rank you should contact Legal Services or RIPA Coordinator for advice.

Time Limits

The current time limits for an authorisation are 3 months for Directed Surveillance and 12 months for a CHIS (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.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire 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 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) that arrangements exist for the source's case that satisfy the requirements of subsection (5) and such other requirements as may be imposed by order made by the Secretary of State. “

Please consult Flowchart 5 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 within 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. Unlike Directed Surveillance, the grounds for authorising a CHIS did not change on 1 November 2012.

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 3.6) 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;
- whether the conduct to be authorized will have any implications for the private and family life to others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

3. Security and Welfare Arrangements

CHISs are often placed in difficult and sometimes 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:

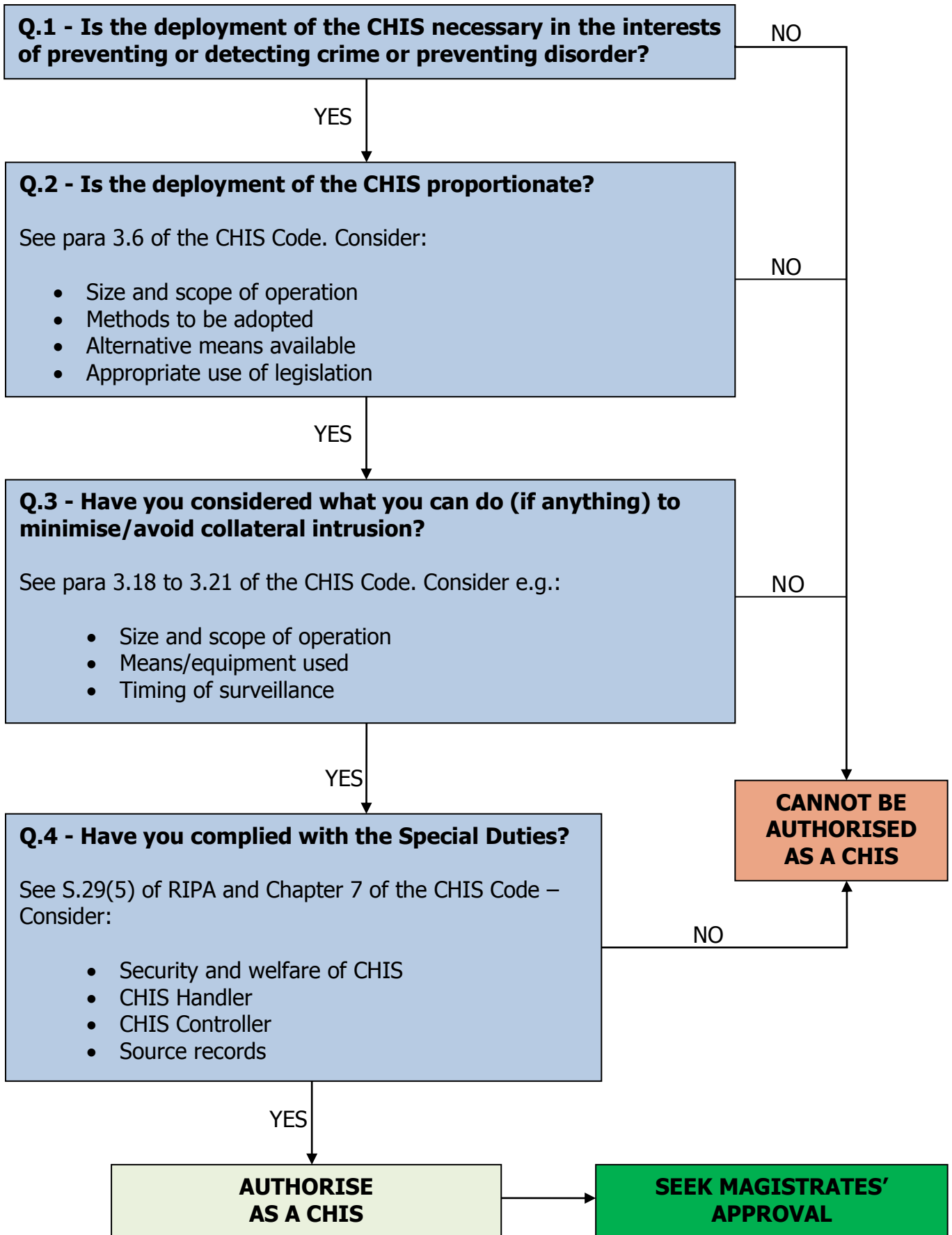
- A person who will have day-to-day responsibility for dealing with the CHIS on behalf of that authority, and for his/her security and welfare;
- A person who will have general oversight of the use made of the CHIS. This person must be different to the one above.
- A person who will maintain a record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

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 CHISs welfare, and, if it is, has given particular consideration to whether the authorisation is justified in the light of that fact.

Flowchart 5 - Authorising a CHIS



PROCEDURE FOR COMPLETING THE RIPA FORMS

The standard forms with guidance notes are on the intranet, in the same section as this Policy (Legal Services, Key Documents). Each standard Home Office RIPA form is reproduced with guidance notes in **dark blue 12 point Calibri font**. These forms are the latest versions downloaded from the Home Office RIPA website.

The Home Office states that public authorities may use these forms or adapt them, for example to include corporate logos or images or to combine review and renewal, or renewal and cancellation forms. However, if they adapt these forms for their own purposes - to record extra information that is not strictly necessary to ensure and demonstrate compliance with RIPA - that additional local requirement should be indicated as being distinct from the necessary recording of RIPA considerations and decisions. On no account though should the forms be pre completed with standard wording, as each application should be made with the specific circumstances of the investigation in mind.

What to do

1. Decide what types of surveillance you are doing (refer to the guidance in Section 2 of this procedure).
2. Use this guidance and associated precedents to complete the appropriate forms. The following documents will also assist in this task:
 - a) The Covert Surveillance and Property Interference Code of Practice
 - b) The Covert Human Intelligence Sources Code of Practice
 - c) The OSC Procedures and Guidance Document – (available from the RIPA Co-coordinator).
3. Once completed, the forms should be sent to the most appropriate authorising Officer for approval. A list of Authorising Officers is available from the SRO.
4. The Authorising Officer should be reminded to read Section 3 of this procedure before completing his/her sections of the form. All authorisation forms should be signed in hard copy by the authorising officer, as opposed to any system of using an electronic signature.
5. If you are seeking a new authorisation or renewing an existing one, remember that it cannot take effect until a Magistrate has approved it. The procedure for this is set out in Section 4 of this document.
6. The original of each completed form (including cancellation forms) should be sent to the RIPA Coordinator who maintains the Council's Central Record of Authorisations, with a copy kept on the operational file.

COMMON MISTAKES IN RIPA FORMS

(Highlighted by the IPOC)

Officers should be aware of the following mistakes when they undertake their respective roles in the RIPA process.

Investigating Officers' Mistakes

- Using of out of date Home Office forms
- Not quoting a unique reference number (URN)
- Copying (cutting and pasting) wording from old authorisation forms
- Failing to give a detailed explanation of what the surveillance will involve
- A surfeit of surveillance tactics and equipment being requested and granted but rarely fully used when reviews and cancellations are examined
- Failing to consider and/or explain the proportionality factors
- Poor and over-formulaic consideration of potential collateral intrusion and how this will be managed
- Failing to consider likelihood of obtaining Confidential Information
- Failing to recognise or be alive to the possibility that someone may have met the CHIS criteria
- Failing to authorise a CHIS promptly as soon as they have met the criteria
- Over-generic risk assessments for a CHIS and not updated to enable the Authorising Officer to identify emergent risks
- Failing to send completed forms to the RIPA Coordinator

Please also read paragraph 4.40 and 4.41 of the Covert Surveillance and Property Interference Code which sets out best working practices with regard to all applications for authorisations under RIPA.

Authorising Officers' Mistakes

- Too many Authorising Officers within the Authority
- Repetitive narrative and rubber stamping without proper consideration of all the facts set out in the authorisation form
- Not knowing the capability of the surveillance equipment which is being authorised. (For instance, there are differences between video cameras that record continuously and those activated by motion; and between thermal image and infrared capability. These differences may have an important bearing on how a surveillance operation is conducted and the breadth of the authorisation being granted. Therefore, a simple authorisation for 'cameras' is usually insufficient)
- Failing to demonstrate that less intrusive methods have been considered and why they have been discounted in favour of the tactic selected

- Discussions that take place between the Authorising Officer and those charged with the management of the CHIS under section 29(5) of RIPA are not always captured in an auditable manner for later recall or evidence
- At cancellation, a lack of adequate, meaningful update for the Authorising Officer to assess the activity conducted, any collateral intrusion that has occurred, the value of the surveillance and the resultant product; with, often a similarly paltry input by Authorising Officers as to the outcome and how product must be managed
- Failing, when cancelling authorisations, to give directions for the management and storage of the product of the surveillance
- No robust management and quality assurance procedures including no regular audits

4. SEEKING MAGISTRATES' APPROVAL

4. GUIDE TO SEEKING MAGISTRATES' APPROVAL FOR RIPA 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 changes the procedure for the authorisation of local authority surveillance under the Regulation for Investigatory Powers Act 2000 (RIPA).

From 1st November 2012 local authorities are required to obtain the approval of a Justice of the Peace (JP) for the use of any one of the three covert investigatory techniques available to them under RIPA namely Directed Surveillance, the deployment of a Covert Human Intelligence Source (CHIS) and accessing communications data.

An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the JP 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 JP to consider either cancellations or internal reviews.

Home Office Guidance

The Home Office has published guidance on the Magistrates' approval process both for local authorities and the Magistrates' 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.

For a brief summary of the approval process please see flowchart 6 at the end of this section.

The New Magistrates' 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 is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP. Authorisation forms will be quality assured by Legal Services. A member of Legal Services will also attend at the Magistrates Court to present the application.
3. The Home Office suggests that the investigating officer will be best suited to making the application for Judicial Approval, although the Authorising Officer may also want to attend to answer any questions.

4. The local authority will provide the JP with a copy of the original RIPA authorisation. This forms the basis of the application to the JP and should contain all information that is relied upon. In addition, the local authority will provide the JP with two copies of a partially completed judicial application/order form (which is included in the Home Office Guidance) (***see the next section for an example with notes to assist completion***).
5. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation and the judicial application/order form. He/She 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 JP will consider whether he or she is satisfied that, at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. He/She will also consider whether there continues to be reasonable grounds. In addition, the JP must be satisfied that the Authorising Officer was of an appropriate level 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 JP and will be the official record of his/her decision. The local authority will need to retain a copy of the form after it has been signed by the JP.

Magistrate's Options

The JP may decide to:-

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

The grant/renewal of the authorisation will then take effect and the local authority may proceed to use the surveillance technique mentioned therein. A copy of the order must be kept on the central record of authorisations.

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

The RIPA authorisation will not take effect and the local authority may not use the surveillance technique in that case. The authority 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 authority can then reapply for Magistrates' approval.

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

A JP may refuse to approve the grant or renewal of an authorisation and decide to quash the original authorisation. This may be because he/she believes it is not necessary or proportionate. The RIPA authorisation will not take effect and the local authority may not use the surveillance technique in that case. The JP must not exercise his/her 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

A local authority may only appeal a JP'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 JP'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.

**Application for Judicial Approval for Authorisation to Obtain or Disclose
Communications Data To Use a Covert Human Intelligence Source or To Conduct
Directed Surveillance
Regulation of Investigatory Powers Act 2000 - Sections 23A, 23B, 32A, and 32B**

Local Authority:

Local Authority Department:

Offence under investigation¹:

.....

Address of premises or identity of subject:²

.....

Covert technique requested: (tick one and specify details)

Communications Data

Covert Human Intelligence Source

Directed Surveillance

Summary of details³

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Note: this application should be read in conjunction with the attached RIPA authorisation/
RIPA application or notice.

Investigating Officer:

Authorising Officer:

Officer(s) appearing before JP ⁴:

Address of applicant department:

.....

Contact telephone number:

Contact email address (optional):

Local authority reference:

Number of pages:

To be completed by local authority

Order overleaf

⁵Order Made on an Application for Judicial Approval for Authorisation to Obtain or Disclose Communications Data, To Use a Covert Human Intelligence Source or To Conduct Directed Surveillance.

Regulation of Investigatory Powers Act 2000 - Sections 23A, 23B, 32A, 32B

Magistrates' Court:

Having considered the application, I (tick one):

am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

⁶refuse to approve the grant or renewal of the authorisation/notice.

⁷refuse to approve the grant or renewal and quash the authorisation/notice.

Reasons

.....
.....
.....
.....

Notes

.....
.....
.....
.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

5. NOTES TO ASSIST COMPLETION - MAGISTRATES' APPROVAL

Notes to Assist Completion

¹Insert the offence or disorder that you are investigating. If you are seeking authorisation for Directed Surveillance make sure that the criminal offence you are investigating attracts a maximum custodial sentence of six months or more or relates to the underage sale of alcohol or tobacco (as per the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012).

²You may not know the identity of the person in which case you can include a description and/or how they relate to the offence/disorder under investigation.

³This forms the basis of the application to the JP and should contain all information that is relied upon. You may wish to set out in brief:

- What information you are seeking from the surveillance
- What the surveillance will involve e.g. covert cameras, CHIS
- How long the surveillance will last

You do not need to go into a lot of detail as this form should have the original authorisation form attached.

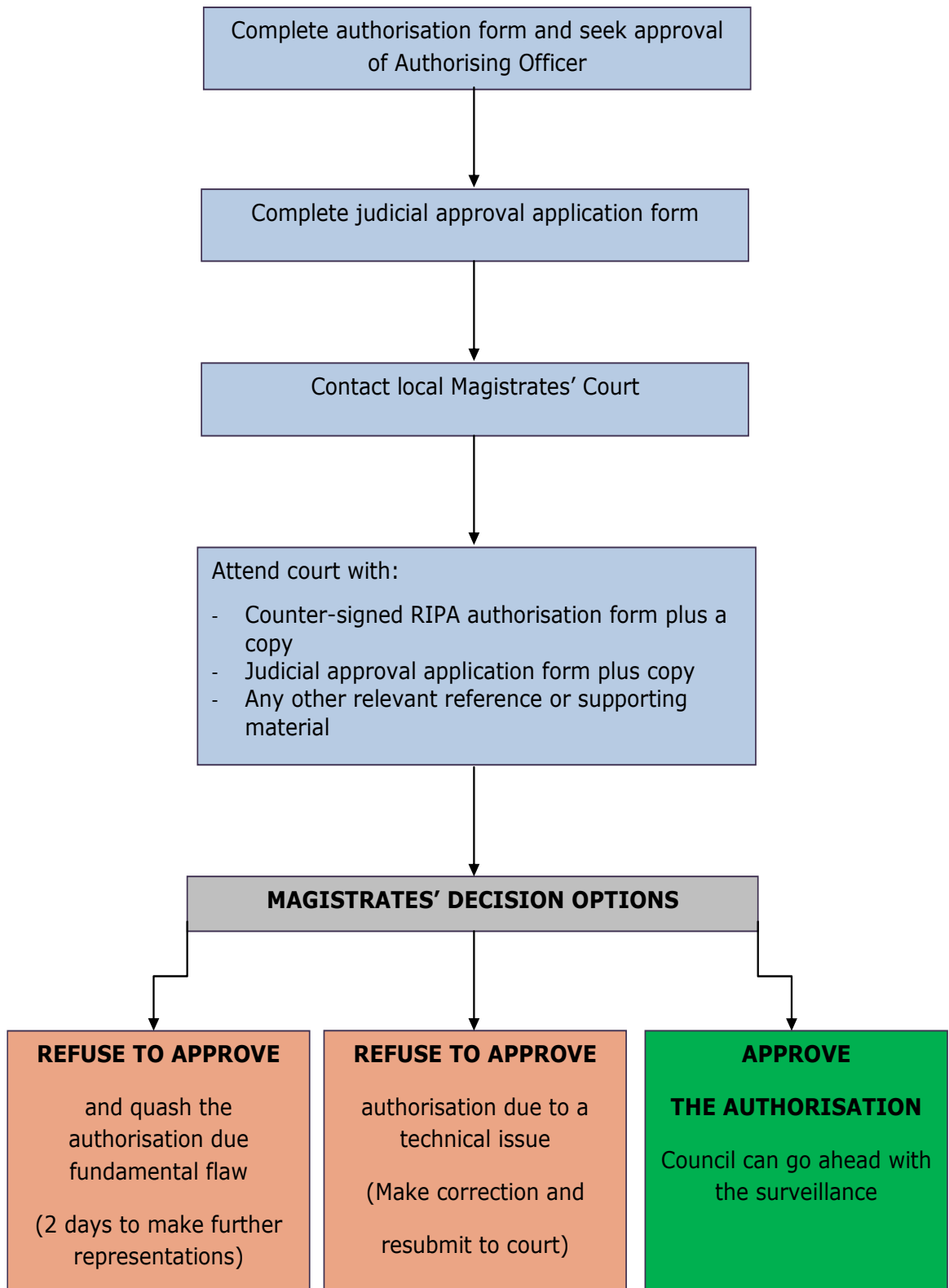
⁴ Any officer employed by the Council can appear before the Magistrate. The Home Office suggests that the Investigating Officer is best placed to do this. Make sure that whoever appears is formally designated to do so under section 223 of the Local Government Act 1972. Legal Services will carry out the initial applications.

⁵The order section of this form will be completed by the Magistrate and will be the official record of the Magistrate's decision. The Council will need to retain a copy of the judicial application/order form after it has been signed by the Magistrate. This may be kept with the original authorisation on the Central Record.

⁶If the Magistrate refuses to approve the authorisation, surveillance cannot be undertaken. This may be due to a technical error which can be corrected. Read the reasons for refusal and seek advice from the Legal Dept. and/or RIPA Coordinator with regards to the next steps.

⁷If the Magistrate decides to quash the authorisation, surveillance cannot be undertaken. You will have two days to make further representations. Read the reasons for refusal and seek advice from the Legal Dept and/or RIPA Coordinator with regards to the next steps.

Flowchart 6 - The Magistrates' Approval Process



6. Governance Arrangements & Quality Assurance

Senior Responsible Officer

Pursuant to the revised Code of Practice the Authority's Senior Responsible Officer is the Assistant Director of Legal Services. The Senior Responsible Officer is responsible for:

- the integrity of the process in place within the public authority to authorise directed and intrusive surveillance;
- compliance with the law and the Revised Codes of Practice;
- oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections;
- where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Judicial Commissioner, and
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

The current list of Authorising officers is as follows:

Sam Barstow (Assistant Director of Community Safety and Street Scene)
Lewis Coates (Service Manager for Regulation and Enforcement)
Alan Pogorzelec (Licensing Manager)
David Webster (Head of Internal Audit)

The SRO will maintain an up to date list of Authorising officers which accurately reflects any changes to personnel and Authorising officers between the annual settings of this policy by elected members. The SRO also regularly monitors the quality of the authorisations forms which are completed, in conjunction with the RIPA Coordinator as part of the overall Quality Assurance process.

Members Oversight

Pursuant to the revised Code of Practice for Covert Surveillance and Property Interference at paragraph 4.47 elected members of a local authority should review the authority's use of the Act and set the policy at least once a year. They should also consider internal reports on use of the Act on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. This is done by means of six monthly reports to the Audit Committee.

Quality Assurance

Quality Assurance will be provided on an ongoing basis by Legal Services who will review and assess all forms as part of the Judicial Approval application process. Feedback will be given directly to relevant officers, with wider feedback given and changes to the Policy made if necessary.

Monitoring and Quality Control

In addition to the Quality Assurance set out above as part of the Judicial Approval application process, the RIPA Coordinator will monitor on receipt the authorisation, renewal, review and cancellations forms which are submitted for the Central Register. Any issues arising from these forms will be brought to the attention of the applying and authorising officer.

The RIPA Co-ordinator

The RIPA Coordinator for Rotherham is Bal Nahal, Head of Legal Services.

Contact details are:-

Phone: 01709 823661

E-mail: bal.nahal@rotherham.gov.uk

The RIPA Coordinator will maintain a register centrally of all authorisations, refusals, reviews, renewals and cancellations. As part of the Judicial Approval application the RIPA Coordinator will monitor the authorisation forms submitted. Further the RIPA Coordinator will monitor on receipt all renewal, review and cancellation forms which are submitted for the Central Register. Any issues arising out of these forms will be brought immediately to the attention of the applying and authorising officer.

IT IS IMPORTANT that all Services keep the RIPA Coordinator updated on all or any changes to authorisation forms.

The RIPA Co-ordinator will keep the records for 5 years to comply with Home Office guidance.

The further responsibilities of the RIPA Coordinator are:-

- a) Oversight of the submitted RIPA documentation
- b) Organising a RIPA training programme
- c) Raising RIPA awareness within the Council

Storage of Authorisation Forms

Each Assistant Director whose department conducts surveillance is responsible for organising sufficient systems within their service in respect of the storage of files and associated RIPA forms.

Copies of the forms should be retained on the operational file for the investigation. The RIPA Coordinator should be sent originals of all authorisations, refusals, reviews, cancellations and renewals of authorisations to satisfy Home Office Code of Practice recommendations.

The following should also be kept by the authorising officer. There is no requirement for this to form part of the central register maintained by the RIPA Coordinator (although pursuant to the current arrangements the originals of forms will be kept by the RIPA Coordinator):-

-
- the original forms of application, authorisation and supplementary documentation and notification of approval given by the authorising officer.
 - a record of the period over which the surveillance has taken place
 - frequency of reviews prescribed by the authorising officer
 - a record of the result of each review of an authorisation
 - a copy of any renewal of an authorisation, and supporting documentation submitted when it was requested.
 - the date and time any instruction was given by the authorising officer.

THE OVERSIGHT OF RIPA

RIPA is overseen by surveillance commissioners. They are tasked to ensure that RIPA is being applied properly. Inspections can be carried out at regular intervals.

Also, any person aggrieved by the way a local authority carries out covert surveillance as defined by RIPA can make a complaint to the Investigatory Powers Tribunal under the Act for redress within a year of the act complained of or any longer period that the tribunal thinks it just and equitable to allow.

This tribunal can quash any authorisation and can order the destruction of information held or obtained in pursuit of it. It can also award damages if it believes that an individual's human rights have been violated by the local authority.